UNIVERZITET CRNE GORE

ELEKTROTEHNIČKI FAKULTET

Jusuf Šabović

ANALIZA BEZBJEDNOSNIH RIZIKA PRI UPOTREBI QR KODOVA – STUDIJA SLUČAJA: FIŠING NAPADI

-master rad-

Podgorica, 2024.

UNIVERZITET CRNE GORE

ELEKTROTEHNIČKI FAKULTET

Jusuf Šabović

ANALIZA BEZBJEDNOSNIH RIZIKA PRI UPOTREBI QR KODOVA – STUDIJA SLUČAJA: FIŠING NAPADI

-master rad-

Podgorica, 2024.

PODACI I INFORMACIJE O STUDENTU

Ime i prezime:	**Jusuf Šabović**
Datum i mjesto rođenja:	26.09.1999. Plav.
Naziv završenog osnovnog studijskog programa i godina završetka studija:	Studijski program Primijenjenog računarstva, Elektrotehnički fakultet, Univerzitet Crne Gore, 180 ECTS kredita, 2021. godine.

INFORMACIJE O MASTER RADU

Naziv master studija:

Analiza bezbjednosnih rizika pri upotrebi QR kodova – studija slučaja: fišing napadi

Naslov rada:	
Alati za testiranje i otkrivanje grešaka u Web aplikacijama: Studija slučaja Upotreba Selenium alat	
Fakultet na kojem je rad odbranjen:	Elektrotehnički fakulte

UDK, OCJENA I ODBRANA MASTER RADA

Datum prijave magistarskog rada:	17.11.2023
Datum sjednice Vijeća na kojoj je prihvaćena tema:	01.12.2023
Komisija za ocjenu/odbranu rada:	Prof. dr Budimir Lutovac, ETF Podgorica, predsjednik Prof. dr Nikola Žarić, ETF Podgorica, mentor Prof.. dr Milutin Radonjić, ETF Podgorica, član
Mentor:	Prof. dr Nikola Žarič
Datum odbrane:	

Ime i prezime autora: Jusuf Šabović, BApp

ETIČKA IZJAVA

U skladu sa članom 22 Zakona o akademskom integritetu i članom 18 Pravila studiranja na master studijama, pod krivičnom i materijalnom odgovornošću, izjavljujem da je master rad pod naslovom

"Analiza bezbjednosnih rizika pri upotrebi QR kodova – studija slučaja: fišing napadi "

moje originalno djelo.

Podnosilac izjave,

Jusuf Šabović, BApp

Jusuf Šabović

U Podgorici, dana 01.11.2024. godine

Izvod teze

Ovaj rad analizira bezbjednosne rizike koje donose QR kodovi. Opisuje se princip rada QR koda, njegov istorijat, način kodiranja i upisivanja informacija, te algoritam koji skeneri koriste pri dekripciji QR koda. Takođe su objašnjeni principi rada jednodimenzionalnih BAR kodova i dvodimenzionalnih QR kodova.

Rad takođe objašnjava fišing napade, najpopularniji hakerski napad u svijetu, kojim svake godine bude "napadnuto" više miliona korisnika Interneta, a mnogi od njih postanu žrtve, čime eksponiraju svoje privatne podatke opasnosti.

Prve dvije funkcionalne cjeline povezane su izvršenim anketnim ispitivanjem 140 korisnika Interneta koji su davali odgovore o iskustvima vezanim za upotrebu QR kodova, hakerske napade i svjesnost o ovoj temi.

Rad zaokružuje eksperimentalni dio koji praktično prikazuje kako QR kodovi mogu biti lako sredstvo za fišing, te kako haker kroz nekoliko linija malicioznog koda može prikupiti informacije o korisniku koji skenira QR kod.

Abstract

This paper analyzes the security risks posed by QR codes. It describes the working principle of QR codes, their history, the method of encoding and embedding information, and the algorithm used by scaners for QR code decryption. The principles of one-dimensional BAR codes and two-dimensional QR codes are also explained.

The paper further explains phishing attacks, the most popular hacking attack worldwide, which affects millions of Internet users anually, with many falling victim and exposing their private data to danger.

The first two functional sections are conected through a survey conducted with 140 Internet users, who provided responses regarding their experiences with QR codes, hacking attacks, and awareness of this issue.

Finally, the paper includes an experimental section that practically demonstrates how QR codes can be an easy tool for phishing, and how a hacker can collect information about the user who scans the QR code through a few lines of malicious code.

Lista slika

Lista tabela

Lista grafikona

Sadržaj

Uvod

QR kodovi su u posljednjih nekoliko godina doživjeli značajan porast popularnosti u gotovo svim djelatnostima, a naročito u naučnom, marketinškom i poslovnom svijetu. Skeniranje QR koda pomoću kamere na mobilnom telefonu postalo je dominantno sredstvo za jednostavan i brz pristup različitim sadržajima poput marketinških kampanja, poslovnih i drugih aplikacija, različitih registracija na veb platfromama itd.

Ovaj trend, najprije zbog svoje jednostavnosti, donosi veliki broj benefita, ali u isto vrijeme otvara vrata novim bezbjednosnim rizicima korisnicima Interneta. Rastom popularnosti QR koda kao efikasnog sredstva u pristupanju raznim Internet sadržajima, a koji nerijetko zahtijevaju i osjetljive podatke na formama za prijave, ili instaliranje aplikacija sa neprovjerenih izvora (najčešće iz pretraživača), porasla je i opasnost po korisnike na mreži. QR kodovi, iako izuzetno efikasni i jednostavni upravo iz tog razloga, postali su pravo (novo) sredstvo za zlonamjerne napade, a pogotovo za fišing.

Istraživanje predstavljeno u ovom radu sagledava različite aspekte bezbjednosnih rizika pri skeniranju QR kodova, i pruža uvid u ponašanje korisnika u vezi sa njima.

Predmet istraživanja

Glavni cilj istraživanja je analiza QR kodova i hakerskih napada kao dvije međusobno povezane komponente u kontekstu informacione sigurnosti.

Sa jedne strane istraženi su QR kodovi kroz njihovo formiranje, popularnost, upotrebu i funkcionalnost, te način na koji se očitavaju na različitim uređajima uz poseban naglasak na način njihove implementacije i učitavanja preko kodova napisanih u programskom jeziku Python.

S druge strane, istražena je tema fišinga kao metode zlonamjernog pristupa informacijama korisnika na Internetu. Istražujući različite metode i tehnike manipulacije kojima se korisnici navode na skeniranje QR koda koji sadrži maliciozni link za preuzimanje aplikacije ili ostavljanje ličnih podataka, uočena je direktna povezanost QR kodova i fišing napada. U programu koji je kreiran za očitavanje QR kodova simuliran je dio malicioznog koda koji bi zlonamjerni hakeri potencijalno mogli da implementiraju u QR kod ili čitač QR koda.

Konačno, imajući u vidu da su, kako QR kodovi tako i fišing duboko ukorijenjeni u socijalni kontekst, istraživanje se bavi analizom bihejviorističkog faktora. Uporednom analizom rezultata

ankete i eksperimenta koji su sprovedeni u sklopu rada, prikazani su rezultati realnog ponašanja korisnika na Internetu i koliki je bezbjednosni rizik od različitih oblika hakerskih napada povezanih sa skeniranjem QR kodova.

Motivi i ciljevi istraživanja

QR kodovi često korisnike upućuju na veb lokacije gdje treba da unesu svoje podatke poput podataka sa bankovnih kartica ili lozinki, ili na lokacije za preuzimanje aplikacija. Upravo ove radnje predstavljaju najveću opasnost po korisnike, jer mogu biti žrtve hakerske prevare. QR kodovi, iako efikasni i jednostavni za upotrebu na ovaj način postali su potencijalno sredstvo za različite oblike cyber napada, a fišing se u tom kontekstu izdvaja kao najrasprostranjeniji.

Ovo istraživanje ima za cilj analizu različitih aspekata rizika po bezbjednost korisnika Interneta, a koji su povezani sa skeniranjem QR kodova, pri čemu su fišing napadi iskorišćeni za studiju slučaja. Svrha rada mogla bi se definisati kao dublji uvid u prirodu i samu ozbiljnost ovih prijetnji na osnovu analize djelovanja i same upućenosti korisnika na njih.

Ključni razlozi i motivi istraživanja su:

- Aktuelnost teme – porast popularnosti QR kodova,
- Polazna hipoteza – nedostatak svijesti o sigurnosti i opasnostima koje kriju QR kodovi,
- Efikasnost napada putem QR kodova,
- Potreba za razvijanjem sigurnosnih mjera,
- Zaštita privatnosti podataka,
- Razvoj sigurnosnih politika i praksi.

Ciljevi istraživanja su:

- Analiza prirode i mehanizama fišing napada putem QR kodova,
- Identifikacija ranjivosti i rizika,
- Procjena učinkovitosti postojećih sigurnosnih mjera,
- Edukacija i podizanje svijesti o vaznosti teme.

Pregled dosadašnjih istraživanja

Autori istraživanja [1] istražuju tehnologiju QR kodova, njihove benefite i potencijalna područja za korišćenje sa aspektom na njihov uticaj u marketinškom i tehnološkom svijetu. Oni navode da

su inicijalno QR kodovi osmišljeni i korišteni u supermarketima, ali danas su postali izuzetno popularni, te gotovo da ne postoji postoji oblast u kojoj nisu našli primjenu. Zbog mogućnosti koje pružaju poput brzog skeniranja, velikog skladišnog kapaciteta i korekcija greški, prema mišljenju autora QR kodovi su doživjeli ovakav rast.

Prema riječima autora istraživanja [2], u septembru 2011. godine je otkriven prvi maliciozni QR kod. Ovaj napad izveden je tako što je korisnik skenirao QR kod i direktno bio preusmjeren na maliciozni veb sajt, a nakon toga su na njegovom uređaju počeli da se instaliraju maliciozni fajlovi, a da to korisnik uopšte nije znao.

Autor istraživanja [3] ilustrovao je generisanje QR kodova i njihovo uključivanje u implementaciju sigurnosnih funkcija u bilo koju aplikaciju konvertujući URL u QR kodove. Autor navodi da se u istoj ravni sa razvijanjem QR kodova moraju razvijati i sigurnosnosni standardi kad su oni u pitanju i da će se u bliskoj budućnosti ova tehnologija koristiti u gotovo svim javnim domenima.

Autorke istraživanja [5] govore o marketinškim i poslovnim potencijalima QR kodova, navodeći primjere da QR kodovi nude korisnicima mogućenost da veoma brzo i jednostavno dobiju sve željene informacije o proizvodima. Autorke takođe navode da QR kodovi moraju u budućnosti biti integrisani u marketing prozivoda ili u brend strategiju ukoliko proizvođači žele da steknu povjerenje i da "se povežu" sa korisnicima.

Popularnost QR kodova razvija se istovremeno sa razvojem popularnosti pametnih telefona, međutim, napadači su počeli koristiti QR kodove za svoje fišing napade koristeći neke od mogućnosti QR kodova. Oni opisuju novi pristup po imenu „Trust QR“, koji koristeći specifične QR komponente kao i specifične komponente URL linkova detektuje da li QR kod sadrži fišing URL. Neki od korištenih komponenti u ovom prepoznavanju mogu biti dužina i tip QR koda.[5]

QR kodovi su sredstvo koje može pomoći edukativnim procesima da isprate tehnološke trendove i inovacije, ali i značajno skratiti vrijeme koje se u toku predavanja troši na podjelu literature. Autori istraživanja navode QR kodove kao idealno sredstvo za automatizaciju procesa predavanja i širenja gradiva, što prilično skraćuje vrijeme koje profesor troši na ovaj segment.

Autori istraživanja [12] prezentuju svoje rješenje koje detektuje fišing veb sajtove. Njihovo rješenje – CANTINA koja koristi "Robust Hyperlinks", koncept za prevazilaženje problema sa stranicama koje se ne mogu pronaći, primjenjujući algoritam Term Frequency / Inverse Document Frequency (TF-IDF) za borbu protiv fišinga. Autori opisuju kako implementirati

CANTINA i prikazuju njegovu evaluaciju pozivajući se na rezultate da TF-IDF algoritam može otkriti oko 97% fišing veb stranica sa oko 6% lažnih pozitiva.

Postoji još dosta prostora za napredak kada je sigurnost QR kodova u pitanju, kao što navode autori istraživanja [13] i predlažu nove bezbjedonosne standarde poput simetrično enkriptovanih QR kodova i QR kodova sa enkripcijom javnog ključa.

Autori istraživanja [14] navode da je prijetnja koju donose fišing napadi uglavnom posljedica ljudskih grešaka. Napadači koriste ljudske i tehničke ranjivosti kako bi izvršili napade. Na podložnost napadima utiču različiti faktori poput starosne dobi, pola, zavisnosti o Internetu, stresa korsnika itd. Autori istražuju nove aspekte fišing napada i predstavljaju anatomiju koja opisuje kompletan životni ciklus jednog napada, kojom pružaju širi pogled na prijetnju i tačniju i potpuniju sliku o načinu funkcionisanja napada.

Autor istraživanja [15] vidi veoma široku upotrebu QR kodova u svakodnevnom životu i istražuje sigurosne probleme povezane sa njima. Autor utvrđuje da postoje korisnici koji skeniraju QR kodove bez razmišljanja o bezbjednosnim posljedicama koje skeniranje zlonamjernog QR koda može da izazove.

Naučne metode i istraživačka pitanja

U radu su dati odgovori na sljedeća istraživačka pitanja:

- Koje vrste napada mogu da se sprovedu putem QR kodova i koje potencijalne rizike donose?
- U kojoj mjeri nedovoljna informatička pismenost može biti uzrok zloupotrebe fišinga putem QR kodova i kako ona može uticati na širenje bezbjednosnih rizika?
- Na koji način se različiti hakerski napadi mogu implementirati kroz QR kod?

Za testiranje i dokazivanje istraživačkih pitanja u vezi sa QR kodovima i njihovom potencijalnom opasnošću od fišinga iskorišćene su različite naučne metode uključujući sljedeće:

- Anketiranje korisnika. Osnovna opasnost od razvoja QR kod fišinga su zapravo korisnici i njihova informatička (ne)pismenost i neopreznost. Anketiranjem određenog broja korisnika mobilnih telefona stečena je slika o realnoj opasnosti koju ova pojava nosi.
- Analiza i obrada podataka. Analiziranjem podataka dobijenih putem anketiranja, ali i podataka koje je moguće pronaći na Internetu, utvrđena je razlika opasnosti od ovakve vrste hakerskih napada u svijetu i u Crnoj Gori.

- Tehnički eksperiment. Upotrebom odgovarajućeg programskog jezika (Python) napisan je kod koji se koristi u skeniranju QR koda. U isti kod moguće je ubaciti malicioznu sekvencu što je i prikazano u eksperimentalnom dijelu rada.
- Sociološki eksperiment. Eksperimentalnim dijelom rada provjerena je lakovjernosti korisnika i prikazan je broj korisnika koji su skenirali neprovjereni QR kod kao i njihovi odgovori.
- Metoda naučnog istraživanja. Ovom metodom je naučno prikazana struktura QR koda u odnosu na različite tipove kao i načini skreniranja, te algoritmi za skeniranje QR kodova.
- Testiranje. Napisani program za skeniranje QR koda je testiran kako bi se utvrdila njegova ispravnost i funkcionalnost.

Rezultati rada

Ovo istraživanje kao rezultat daje uvid u stvarnu i realnu opasnost od hakerskih napada, popularnog fišinga putem QR kodova. Korišćenjem naučnih i istraživačkih metoda u radu se daju odgovori na pitanja: "Da li su, i u kojoj mjeri, QR kodovi bezbjedni za korišćenje", "Koliko je lako manipulisati QR kodovima", "Kolika je svijest korisnika o potencijalnoj opasnosti od upada u privatnost i potencijalnim problemima koje ne samo QR kod fišing, već i ostali sajber napadi mogu prouzrokovati". Posljednje pitanje je pogotovo važno, jer ukoliko na nivou društva ne postoji svjesnost opasnosti od sajber napada onda se QR izdvaja kao najlakši "mamac" koji hakeri mogu iskoristiti u svoju korist.

U radu je, takođe, prikazano kako izgleda struktura koda i algoritama za skeniranje i formiranje QR koda, te na koji način je moguće ubaciti maliciozne sekvence kod kojih se koristi za skeniranje odnosno formiranje QR koda.

Eksperimentom sa statističkim podacima otvaranja neprovjerenog i sumnjivog koda kao i anketom koja je sprovedena u okviru rada dobijena je i prikazana još bolja slika stvarne opasnosti po korisnike.

Rezultati istraživanja bi mogli koristiti strategiji za zaštitu od sajber napada, ali i analitičarima informacione bezbjednosti kako u državnim institucijama tako i u privatnim kompanijama za bolju pripremu strategije. Kao dodatno sredstvo za budući rad na temu, u okviru rada napisana je i prikazana skripta u programskom jeziku Python koja dešifruje QR kod i provjerava da li URL link pripada grupi najpoznatijih fišing URL linkova na svijetu.

Struktura rada

U prvom dijelu rada objašnjen je princip rada QR kodova, objašnjena razlika između jednodimenzionalnih i dvodimenzionalnih bar kodova, te s tim u vezi objašnjen istorijski nastanak QR koda i bar kod. U radu su nabrojani i objašnjeni tipovi QR kodova, njihova struktura i način generisanja kao i način na koji skener čita i dešifruje QR kod.

U drugom dijelu rada objašnjen je fišing napad kao najčešći hakerski napad u svijetu na konkretnim primjerima i podvučena je paralela kako QR kod može biti iskorišćen kao sredstvo za fišing napade. U ovom dijelu rada objašnjeno je i na koji način ostali tipovi hakerskih napada mogu biti izvedeni posredstvom QR koda.

U trećem dijelu rada prikazani su rezultati anketnog istraživanja sprovedenim nad 140 korisnika/ca Interneta koji su davali odgovore o poznavanju QR koda, informacione bezbjednosti i u cijelosti o sigurnosti skeniranja QR kodova.

U posljednjem dijelu rada odrađen je eksperiment sa manipulacijom QR kodom i prikazani su rezultati skeniranja takvog koda.

1. QR kodovi

QR kod je vrsta matičnog bar koda ili dvodimenzionalnog koda koji je dizajniran tako da može biti skeniran pomoću mobilnih telefona. Sadržaj koda bi putem pametnih mobilnih telefona i ostalih pametnih uređaja trebao biti dekodiran velikom brzinom [1].

Vizuelno, kod se sastoji od kvadrata bijele pozadine na kome su raspoređeni crni moduli. Kodirane informacije mogu biti tekst, URL (Uniform Resource Locator – adresa resursa na Internetu) ili drugi podaci poput WiFi (Wireless Fidelity – bežična mreža) mreža, poslovnih informacija ili SMS (Short Message Service – vrsta kratkih poruka) poruka.

Uzimajući u obzir široku rasprostranjenost pametnih uređaja u današnjem svijetu, kao i činjenicu da veliki broj pametnih uređaja ima omogućen pristup Internetu i ugrađenu kameru, popularnost QR kodova rapidno raste u posljednje dvije decenije.

QR kodovi su kreirani 1994. godine od strane Toyota-ine ekspoziture Denso Wave i prvobitno su korišćeni za praćenje inventara u sektoru proizvodnje vozila. Danas se QR kodovi koriste u gotovo svim oblastima ljudske djelatnosti i daleko su šire rasprostranjeni od same proizvodnje motornih vozila [5].

Usljed velike kapacitivnosti pogodne za skladištenje značajne količine podataka, tehnologija dekripcije dvodimenzionalnih kodova napreduje i u smjeru inteligencije, minijaturizacije i umrežavanja što daje ogroman i dugoročan značaj sistemu identifikacije QR slika zasnovanih na vještačkoj inteligenciji.

Slika 1. Primjer QR koda

1.1 Bar kodovi

Bar kodovi su kodovi sastavljeni od crnih i bijelih traka koje se smjenjuju, a njihove širine se obično sabiraju do fiksne širine za sve znakove. Ovim se omogućava skeniranje kompletnog koda prihvatljivom brzinom jer se vremenske širine svake trake mogu izraziti frakcijom vremena koje je potrebno da bi se skenirala kompletna cifra.

Numerički podaci su u bar kodovima predstavljeni nizom traka različite debljine i razmaka, a radi paktičnosti ovi podaci su uglavnom odštampani i prikazani ispod bar koda [18].

Slika 2. Bar kod

1.2 Diskretni (jednodimenzionalni) i dvodimenzionalni bar kodovi

Postoje dvije glavne vrste bar kodova koje se najčešće koriste: diskretni i kontinuirani bar kodovi.

Diskretni bar kodovi (jednodimenzionalni) kodiraju podatke predstavljanjem znakova pomoću različitih širina i razmaka traka. Svaki znak je pojedinačno sastavljen od niza traka i praznina, zauzimajući specifičan prostor duž bar koda.

Najčešće korišćeni diskretni bar kodovi su UPC (Universal Product Code) i EAN (Europian Article Number) i oni se nalaze na proizvodima u prodaji (trgovinama npr.). UPC se koristi u zemljama poput SAD-a, Kanade, Novog Zelanda i Australije za praćenje trgovinske robe u prodaji, odnosno za identifikaciju proizvoda. EAN se koristi u iste svrhe, ali je namijenjen za Evropsko tržište.

Slika 3. Diskretni bar kodovi

Ova vrsta bar kodova pogodna je za kodiranje relativno malih količina podataka kao što su numerički ili alfanumerički identifikatori proizvoda i skeniraju se laserskim skenerima kakve gledamo u trgovačkim lancima. S druge strane, kontinuirani odnosno dvodimenzionalni bar kodovi podatke kodiraju u dva pravca (dimenzije), horizontalno i vertikalno čime omogućavaju gustu pohranu informacija u poređenju sa jednodimenzionalnim. QR kodovi su, dakle, ”ažurirana” verzija jednodimenzionalnih bar kodova osmišljena da ‘’čuvajući’’ informacije u dva pravca (horizontalno i vertikalno), čuva veću količinu podataka i na taj način neutrališe i najmanju mogućnost dekodiranja ljudskim okom [1], [18].

1.3 Istorijat QR kodova

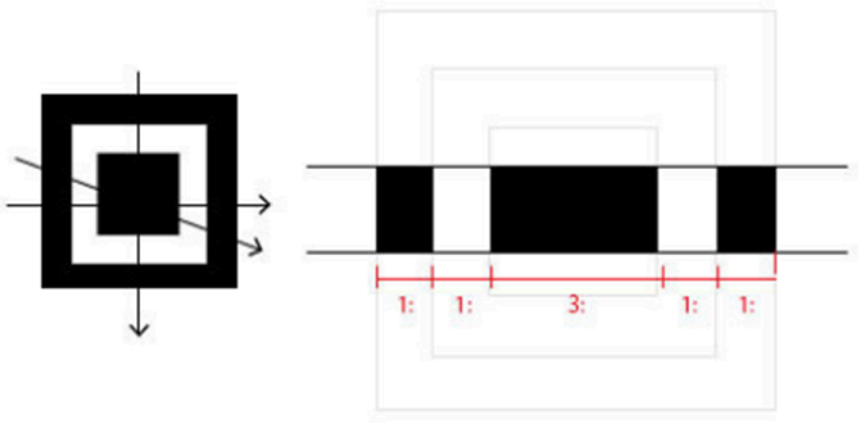
Razvoj QR kodova datira od 1994. godine kada je japanska kompanija Denso Wave (ekspozitura Toyota Grupe), osmislila ovu tehnologiju koja se ubrzo ispostavila revolucionarnom. QR kodovi su prvobitno razvijani u sektoru proizvodnje dijelova za motorna vozila radi lakšeg praćenja, ali su brzo prevazišli ovu upotrebu i proširili se na ostale industrijske grane. Upravo je kompanija Denso Wave osmislila dvodimenzionalne bar kodove koji mogu da sadrže više od 20 alfanumeričkih znakova, grupišući podatke na način da su sličniji jedni drugima.

Na početku je glavni inženjer na projektu Masahiko Hara pokušao da unaprijedi skenere bar kodova, ali je, uvidjevši nedostatke ovih sistema odustao od te ideje. "Razvijamo kompaktni kod koji može skladištiti više informacija, uključujući kanji i kana karaktere i istovremeno može biti čitan većom brzinom.", odlučio je Hara [22].

Najveći izazov u Hara-inom radu bio je omogućavanje brzog čitanja 2D kodova, jer ih je teže čitati nego bar kodove. Hara je došao na ideju da dodavanjem informacija o lokaciji u kod može da riješi ovaj problem. Na taj način je kreirana šema za detekciju pozicije smještena na tri ugla svakog koda. Razvojni tim je, istražujući odnos bijelih i crnih površina u šemama, otkrio da odnos 1:1:3:1:1 najmanje budi sumnju u prepoznavanju.

Razvojni rad je trajao godinu i po dana nakon kojih je sistem QR koda uspješno razvijen. Ovakav kod može skladištiti velike količine informacija i čitati se brzinom većom od deset puta kada se poredi sa drugim kodovima [4].

Slika 4. Kvadrati za detekciju položaja



U svim pravcima odnos crnih i bijelih površina u obrascima za detekciju položaja je 1:1:3:1:1

Slika 5. Odnos crnih i bijelih površina u obrascima

QR kodovi su u Denso Wave-u donijeli još jednu povoljnost – otporni su na prljavštinu i oštećenja što znači da ukoliko su izloženi na primjer ulju ili drugim nečistoćama ili oštećeni u toku proizvodnje i dalje mogu biti skenirani zahvaljujući funkciji za ispravljanje grešaka.

Danas se QR kodovi mnogo šire koriste nego na samom početku. Od lansiranja QR koda, Denso Wave neprestano radi na njihovom unapređivanju. Novi QR kodovi sada imaju SQRC (Skraćeno Eng. Secure QR Code – osigurani QR kod), koji ograničava čitanje podataka i tako povećava sigurnost, ograničavajući pristup podacima samo putem računarskog skeniranja.. Osim SQRC-a, novi QR kodovi danas imaju i frame QR koji poboljšava estetičnost samog QR koda.

"Razvijamo sisteme koji koriste QR kodove iz perspektive korisnika", izjavio je Atsushi Tano, iz grupe za sistemska rješenja kompanije Desno Wave, [22].

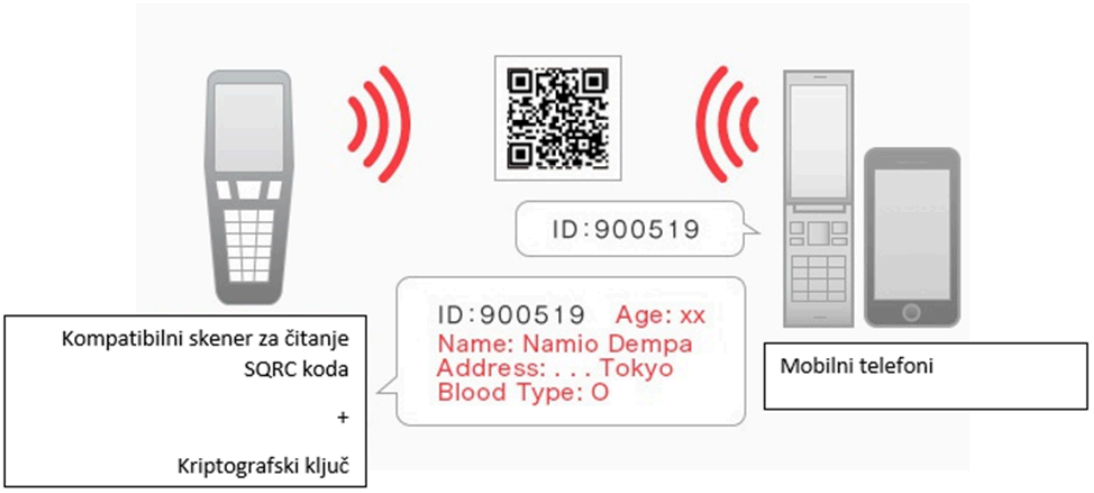
1.4 Tipovi QR kodova

Razvojem tehnologija QR kodova razvilo se i više različitih vrsta i tipova QR kodova usljed različitih industrijskih potreba. Tako je zbog potrebe da se QR kodovi odštampaju u manjim fizičkim veličinama zbog postavljanja na mikro djelove proizvoda nastao Micro QR kod. Ovaj kod može imati širinu od dva modula pri čemu je modul najmanji element – crni ili bijeli ali i dalje može biti upotrebljiv. Moduli kod Micro QR koda su elementi (kvadratići) koji čine uzorak

koda, odnosno svaki od njih predstavlja jedan bit informacija dok njihova kombinacija kodira podatke. Najveća verzija ove vrste koda je M4 koji se sastoji od 17x17 modula i može sadržati do 35 brojeva [16].

Slika 6. Primjer Micro QR koda

Kako bi se obezbjedila sigurnost kojom će se ograničiti čitanje privatnih podataka osmišljen je Sigurnosni QR kod (SQRC). Ovaj kod se koristi za distribuciju privatnih, povjerljivih informacija prema autorizovanim osobama šifrovanjem podataka kako bi samo ovlašćeni korisnici mogli imati pristup informacijama. Šifrovanjem se dobija mogućnost da samo određeni korisnici ili uređaji mogu pristupiti podacima čime se omogućava kontrola pristupa. Na ovaj način se, na primjer, mogu dijeliti lozinke, finansijski podaci ili neki osjetljivi dokumenti [15], [16].



Slika 7. Skeniranje i dekripcija SQRC koda

Kada se SQRC kod skenira standardnim čitačem QR koda, biće pročitan kao i svaki drugi QR kod. Međutim, ključna razlika je u tome što je pročitana poruka zapravo kriptovana i standardni čitači će prikazati šifrovan i besmislen tekst. Da bi se SQRC kod pročitao potreban je poseban i kompatibilan uređaj za čitanje koda koji će dekriptovati i dodatno ekriptovani tekst koristeći ključ za dekripciju podataka nakon čega će biti jasna poruka koja se "krila" iza koda.

U marketinške svrhe osmišljen je Frame QR sa „canvas area" (dio ekrana ili prozora u kome se može umetnuti slika, izraz najčešće korišćen u grafičkom dizajnu), gdje se mogu umetnuti slike, logotipi ili slova.

Slika 8.Primjer frame QR koda

1.5 Funkcionalnosti QR koda

Već je rečeno da QR kodovi skladište informacije u dva pravca – horizontalno i vertikalno što im omogućava kodiranje više informacija u odnosu na jednodimenzionalne bar kodove koji informacije skladište samo horizontalno. QR kodovi koriste različite obrasce kao što su Finder Pattern (obrasci za pronalaženje, služi kao referenca čitačima QR kodova za pravilno čitanje, lociranje i orijentisanje QR koda), Alignment Pattern (obrasci za poravnanje, služi za ispravljanje distorzije QR koda u slučajevima kada se skenira pod različitim uglovima ili sa zakrivljenim površinama), Timing Pattern (obrasci za vremensko određivanje, odnosno određivanje modula u QR kodu) i Quiet Zone (tiha zona, odnosno prazan prostor oko modula QR koda). Ovi obrasci čine QR kodove jednostavnim za brzo i efikasno mašinsko dekodiranje, a nemogućim za dekodiranje ljudskom oku [5], [8].

Među najznačajnijim dodatnim funkcionalnostima dvodimenzionalnih QR kodova u odnosu na jednodimenzionzionalne bar kodove može se navesti mogućnost ispravljanja greške. Ova funkcionalnost omogućava QR kodu da bude otporniji na oštećenja ili ostale neželjene posljedice čime će se povećati mogućnost uspješnosti dekodiranja na skeneru. Ova karakteristika je

posebno doprinijela popularnosti QR kodova, pa se oni danas mogu koristiti u industrijskim postrojenjima, u transportu, ali i na ulici, u svakodnevnom funkcionisanju građana.

Još jedna funkcionalnost koja podiže popularnost QR kodu je mogućnost ugradnje različitih tipova podataka poput teksta, URL-a, kontakt informacija, WiFi mreže, geografske lokacije itd. Ovakva svestranost omogućava da QR kodovi pronađu primjenu u svim sferama današnjeg života. Na primjer, QR kod na reklami može sadržati URL koji vodi do web stranice sa dodatnim informacijama ili se može nalaziti u gradskom prevozu, pružajući podatke o redu vožnje.

Slika 9. Primjer primjene QR koda za vrijeme pandemije virusa COVID-19

1.5.1 Korekcija greške QR koda

Među najznačajnijim dodatnim funkcionalnostima koje sa sobom nose QR kodovi, a što ih čini još popularnijim i svrsishodnijim, je detekcija greške. Kako bi postigao ovu funkcionalnost, QR kod generiše niz ispravljajućih kodova koji su dodati sekvenci podataka. Na taj način omogućava da simbol bude jasan i čitljiv čak i u posebnim uslovima poput oštećenja ili dodira sa prljavštinom. Ova funkcionalnost postiže se korišćenjem Reed-Solomonovih kodova – široko korišćene matematičke metode ispravljanja grešaka. Ova metoda koristi redundantne podatke (višak) dodate originalnom podatku kako bi omogućila rekonstrukciju ispravnog podatka, čak i ako je došlo do grešaka pri prenosu ili skladištenju. Reed-Solomon kodovi se zasnivaju na polinomima. Originalni podaci se predstavljaju kao koeficijenti polinoma. Zatim se dodaju dodatni podaci (redundantni bitovi), koji omogućavaju ispravljanje grešaka. Ovi dodatni podaci su generisani tako da mogu rekonstruisati originalne podatke čak i ako dođe do grešaka u dijelu informacija [3].

Reed-Solomonova metoda koristi Galoisova polja (konačna polja) za rad sa polinomima, što omogućava rad sa binarnim podacima u digitalnim sistemima.

Za polinom definisan sa *k* koeficijenatom, Reed-Solomon kod može ispraviti do *t* grešaka po formuli:

$$n = k + 2t$$

Gdje je *n* ukupna dužina kodne riječi, *k* dužina originalnih podataka, a *t* broj grešaka koje se mogu ispraviti. Ova metoda može ispraviti do *t* grešaka pri čemu je: $t = (n-k) / 2$. [3]

Postoje četiri nivoa detekcije i ispravke greške a viši nivoi imaju veću sposobnost oporavka. U tabeli 1 prikazani su svi nivoi ispravke greške. Na odabir nivoa ispravke greške utiču uslovi okoline kao i željena veličina QR koda.

Tabela 1. Nivoi ispravljanja greške kod različitih tipova QR kodova

Broj	**Nivo ispravljanja greške**	**Procijenjena vjerovatnoća ispravke u procentima**
1	L	7%
2	M	15%
3	Q	25%
4	H	30%

Na realnom primjeru nivoi Q i H koji imaju procijenjenu mogućnost ispravljanja greške od 25 i 30 %, respektivno, će najviše biti zahtijevani pri izradi QR kodova, u, recimo, fabrikama gdje postoji realna vjerovatnoća da će se oštetiti ili isprljati. U ostalim "čistijim" uslovima i u kodovima koji sadrže velike količine podataka češće će se koristiti nivoi M i L sa 7% i 15% mogućnosti korekcije greške [3].

1.6 Primjena QR kodova u praksi

Zbog svoje jednostavnosti i brzine skeniranja, ali i količine podataka koje kriptuje, QR kod je evoluirao od fabrike za proizvodnju djelova automobila do primjene u gotovo svim oblastima života i rada, [5].

Neke od najznačajnijih primjena QR kodova prikazane su u tabeli ispod.

Tabela 2. Primjeri primjene QR kodova u različitim djelovima svakodnevnog života

Primjena	**Primjer**

ZDRAVSTVO	Tokom pandemije virusa COVID-19, mnoge zemlje uvele su obaveznu vakcinaciju kao dio svojih zdravstvenih politika za suzbijanje širenja virusa. Ulazak u većinu javnih i privatnih institucija zahtijevao je potvrdu o vakcinaciji, koja je postala ključni alat u kontroli i praćenju epidemiološke situacije. Validnost tih potvrda provjeravala se skeniranjem QR koda, koji je sadržavao informacije o statusu vakcinacije pojedinca.
TRGOVINA	QR kodovi našli su svoju primjenu i u trgovini, pružajući dodatne informacije i olakšavajući kupcima pristup relevantnim podacima o proizvodima. Iako se bar kodovi još uvijek koriste na kasama za skeniranje cijena i vođenje zaliha, QR kodovi se sve češće nalaze na ambalažama proizvoda. Ovi kodovi omogućuju korisnicima da jednostavnim skeniranjem putem pametnih telefona dobiju detaljne informacije o proizvodu, uključujući specifikacije, dostupnost u radnji, sastav, uputstva za upotrebu i promocije.
PREVOZ	QR kodovi našli su široku primjenu i u sektoru prevoza, značajno unapređujući efikasnost i korisničko iskustvo. Ovi kodovi se koriste za različite svrhe, uključujući izdavanje karata, praćenje tereta i informisanje putnika.
UGOSTITELJSTVO	QR kodovi našli su svoju primjenu i u sektoru ugostiteljstva, unapređujući efikasnost usluga i poboljšavajući iskustvo

	gostiju. Ova tehnologija omogućava gostima pristup širokom spektru informacija i usluga jednostavnim skeniranjem koda putem pametnih telefona.
MARKETING	QR kodovi imaju široku primjenu u marketingu, pružajući inovativne načine za angažovanje potrošača i unapređenje marketinških kampanja. Njihova jednostavna upotreba i sposobnost da brzo prenesu informacije čine ih moćnim alatom za poboljšanje interakcije s kupcima i povećanje konverzija.
WIFI ŠIFRE	QR kodovi našli su svoju primjenu i u povezivanju s WiFi mrežama, pružajući brz i jednostavan način za pristup Internetu bez potrebe za unosom složenih lozinki samo skeniranjem QR koda kamerom mobilnog telefona.
PRAĆENJE INVENTARA	QR kodovi se koriste i u praćenju inventara, omogućavajući precizno i efikasno upravljanje zalihama u različitim industrijama. Korišćenjem QR kodova za praćenje inventara poboljšava se tačnost podataka, smanjuje mogućnost ljudskih grešaka i olakšava upravljanje skladištem.
EDUKACIJA	QR kodovi se danas koriste i u edukativne svrhe, na primjer za pristup dodatnim resursima, video materijalima ili kvizovima.
PLAĆANJE	QR kodovi su sve popularniji u digitalnom plaćanju. Korisnici mogu skenirajući QR kod na kasi ili na računu platiti putem mobilnog

	novčanika ili putem neke od aplikacija za mobilno bankarstvo.
PRIMJENA ZAKONA	U Crnoj Gori od 2021. godine svi fiskalni računi moraju sadržati QR kod kojim korisnici mogu provjeriti da li je došlo do eventualne zloupotrebe pružaoca usluga, odnosno da li je kupovina registrovana – sprečavanje sive ekonomije.

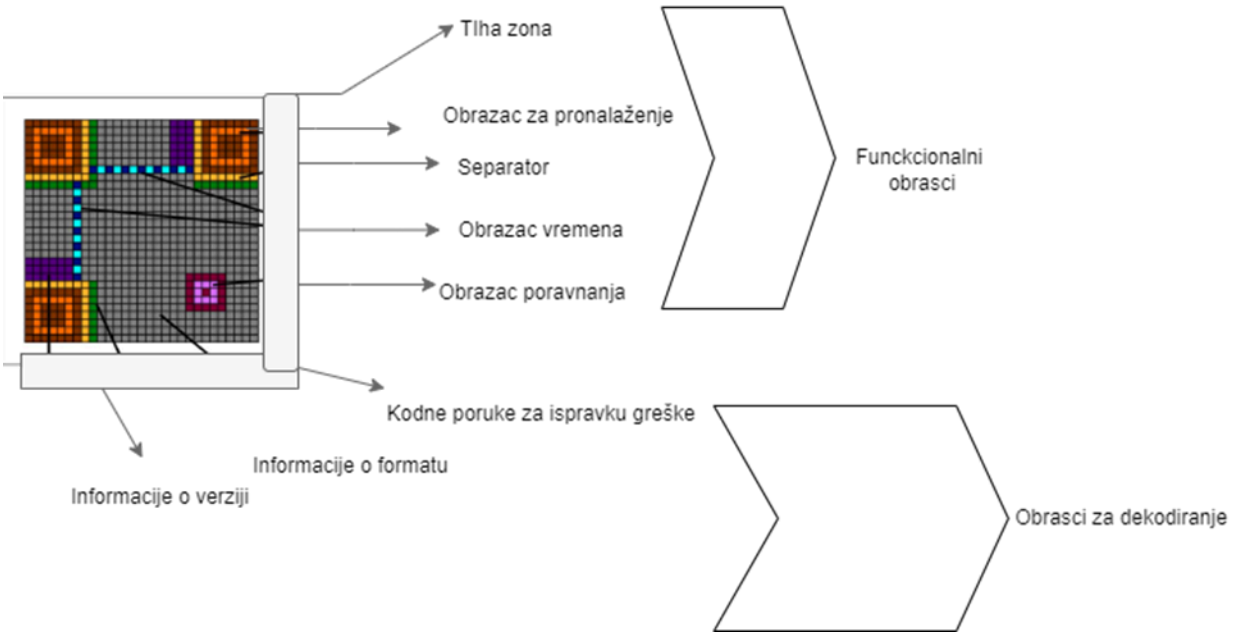
1.7 Struktura QR koda

Svaki simbol QR koda je izgrađen od kvadratnih modula koji su raspoređeni u redovnom kvadratnom nizu i sastoji se od funkcionalnih obrazaca i regiona kodiranja. Čitav simbol bi trebao da bude okružen sa sve četiri strane "mirnom graničnom zonom". Oblici funkcionalnih obrazaca moraju biti postavljeni prema specifičnim oblastima QR koda čime se osigurava da skeneri tačno mogu identifikovati kodne sekvence odnosno izvršiti dekodiranje [3].

Postoje 4 vrste funkcionalnih obrazaca i to:

1. Obrasci pretrage,
2. Separatori,
3. Obrasci sinhronizacije,
4. Obrasci poravnavanja.

Region kodiranja sadrži podatke koji predstavljaju informacije poput verzije, formata poruke, podataka i kodova za ispravku eventualnih grešaka. Struktura QR koda prikazana je na slici 10, [16].



Slika 10. Struktura QR koda

Obrasci pretrage

Obrasci pretrage su posebni obrasci koji služe za detekciju pozicije i locirani su u tri ugla – gornji desni, gornji lijevi i donji lijevi svakog simbola. Sastoje se od spoljnje tamne kvadratne površine dužine 7x7 modula, unutrašnje kvadratne površine koja je svijetla (bijele boje) dužine 5x5 modula, te čvrste tamne kvadratne površine koja se nalazi u centru i dužine je 3x3 modula.

Odnos širina modula u svakom obrascu pretrage je 1:1:3:1:1 kao što je prikazano na slici 5. Ovi obrasci su dizajnirani kao posebni obrasci koji je gotovo nemoguće da se pojave unutar drugih sekcija QR koda, kako bi skener QR koda odmah mogao da traži odnos svijetlih i tamnih modula čime tačno orijentiše QR kod za dekodiranje.

Separatori

Separator je jedno-modularni prostor koji stoji između svakog obrasca pretrage i regiona kodiranja QR koda i razdvaja ih. Separatori pomažu skenerima da prepoznaju QR kod i odrede njegovu orijentaciju stvarajući bijelu granicu oko obrazaca. Obično su bijele boje i debljine jednog modula (kvadratnog elementa) QR koda. Glavna funkcija separatora je da jasno odvoje pozicione obrasce od kodiranih podataka u QR kodu.

Obrasci sinhronizacije

Budući da su QR kodovi dvodimenzionalni (čitaju se i čuvaju podatke u dva pravca – horizontalno i vertikalno), za obije dimenzije postoji obrazac sinhronizacije – horizontalni i vertikalni. Ovi obrasci se sastoje od svijetlih i tamnih modula koji se smjenjuju.

Horizontalni obrazac sinhronizacije je postavljen u šestom redu QR koda između separatora, dok je vertikalni obrazac sinhronizacije postavljen u šestoj koloni QR koda, takođe između sinhronizatora. Oba ova obrasca pomažu u sljedećim aktivnostima:

- Određivanje gustine simbola

Horizontalni i vertikalni obrasci sinhronizacije omogućavaju skenerima da precizno utvrde broj modula u QR kodu što pomaže u određivanju gustine simbola. Ova dva obrasca osiguravaju pravilno poravnanje i dekodiranje QR koda u svim uslovima skeniranja čak i ukoliko postoje distrozije ili varijacije u veličini.

- Koordinata modula

Omogućava skenerima da precizno identifikuju pozicije različitih funkcionalnih obrazaca, očitaju i implementiraju podatke, te identifikuju eventualne greške i isprave ih. Bez ispravnih koordinata pouzdanost i efikasnost QR kodova bila bi značajno umanjena.

- Informacijama o verziji.

Verzija QR koda utiče na broj modula u svakom redu i koloni kao i na količinu podataka koji se mogu kodirati. Verzija određuje dimenziju i kapacitet pohrane podataka. Više verzije omogućavaju veći kapacitet i kompleksnije aplikacije, dok niže nude jednostavnije i kompaktnije rješenje.

Region kodiranja

Region kodiranja sadrži informacije o:

- Formatu

Region kodiranja sadrži informacije o formatu QR koda kroz specifične module uključene u strukturu QR koda. Podaci o formatu QR koda uključuju informacije o nivou korekcije greške (L, M, Q, H). Smješteni su u dva dijela QR koda na način da im skeneri mogu lako pristupiti i pročitati formatne informacije bez obzira na orijentaciju QR koda.

- Verziji

Informacije o verziji QR koda nalaze se u dva dijela koda i prisutne su samo u verzijama QR koda od verzije 7 i više. Manje verzije nemaju zasebne module za informacije o verziji jer su

dovoljno male da je skeneru lako odrediti njihovu strukturu bez dodatnih informacija. Informacije o verziji sastoje se od 18 bitova raspoređenih u dva uzorka veličine 6x3 modula i kodiraju broj verzije QR koda binarnim kodom.

- Kodovima za ispravku grešaka

Region kodiranja sadrži podatke o kodovima za ispravku grešaka kroz proces koji uključuje dodavanje redundantnih podataka pomoću Reed-Solomon algoritma. Ovi kodovi su ravnomjerno raspoređeni po cijelom QR kodu i omogućavaju skenerima da detektuju i ispravljaju greške.

Za informacije o formatu mora da bude rezervisan jedno-modularni niz u blizini gornjeg lijevog, gornjeg desnog i donjeg lijevog obrasca. Dakle, u blizini obrazaca pretrage kao i informacije o verziji, te oblast od 6x3 bloka iznad donjeg lijevog obrasca pretrage i blok 3x6 lijevo od gornjeg desnog obrasca pretrage.

Obrasci poravnanja

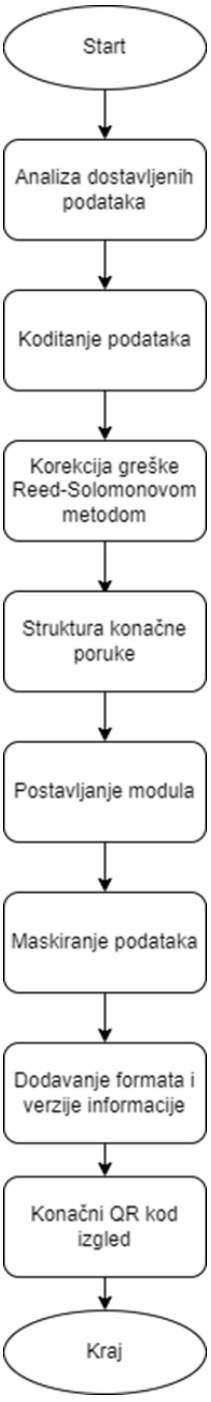
Obrasci poravnanja pomažu u ispravljanju distorzija i osiguravaju preciznost čitanja podataka. Posebno su važni za veće verzije QR kodova gdje postoji veća mogućnost pojave greške u očitavanju zbog distorzija ili zakrivljenosti površine na kojoj je QR kod odštampan ili otisnut. Obrasci poravnanja su manji kvadratići koji se nalaze unutar QR koda. Od verzije 2 svi QR kodovi sadrže jedan ili dva obrasca poravnanja. Ovi obrasci se sastoje od 5x5 tamnih modula, 3x3 svijetlih modula te jednog tamnog modula koji se nalazi u samom centru. QR kodovi koji su verzija 2 ili više moraju imati obrasce poravnanja, a njihov broj zavisi upravo od verzije simbola. Sastoje se od manjeg kvadrata unutar veće bijele zone. Centralni kvadrat je crn "okružen" bijelim moduilima koji su opet okruženi crnim modulima. Prilikom skeniranja obrasci poravnanja omogućavaju čitanje koda, nezavisno od uslova zakrivljenosti ili distorzije.

Tiha zona

Ovo je oblast široka četiri modula koja ne sadrži podatke i koristi se kako bi se osiguralo da ne dođe do miješanja okolnog teksta i podataka koji se nalaze na QR kodu. Ova zona je zapravo prazan prostor i okružuje QR kod, praveći jasnu granicu između sadržaja QR koda i okolnog "prostora". Od izuzetne je važnosti jer omogućava skenerima da pravilno identifikuju granice QR koda i odvoje ga od ostalih međuelemenata. Tiha zona ne sadrži podatke ili uzorke i njena veličina varira u odnosu na veličinu QR koda. Osim što je važna u skeniranju, tiha zona pomaže i u zaštiti QR koda od oštećenja pružajući dodatnu marginu koja štiti osjetljive djelove koda.

1.8 Algoritam generisanja QR koda

Proces generisanja QR kodova sastoji se od osam ključnih koraka. Svaki od ovih koraka mora se izvršiti po tačno određenom redoslijedu, kako bi se osigurala sigurnost i integritet informacija.



Slika 11. Algoritam generisanja QR koda

Analiza dostavljenih podataka

U prvom koraku algoritma za generisanje QR koda fokus je na analizi dostavljenih podataka, kako bi se odredila najbolja strategija kodiranja. Dostavljeni podaci se analiziraju kako bi se odredila vrsta podatka (numerički, alfanumerički, binarni, kanji) [16].

Kodiranje podataka

Nakon što su podaci analizirani i utvrđen je najbolji metod za kodiranje podataka slijedi korak samog kodiranja. U ovom koraku QR kod enkodira niz teksta jednim od četiri režima za enkodiranje koji se koriste:

1. Numerički

Grupisanjem brojeva u grupe od po tri cifre i pretvaranje svake grupe u binarni oblik. Svaka grupa se kodira u 10-bitni niz, a na početku se dodaje prefiks koji označava da je način kodiranja numerički.

2. Alfanumerički

Alfanumerički se kodiraju brojevi i slova kombinovano. Iako je manje efikasan od numeričkog, omogućava širu upotrebu. Znakovi se grupišu po dva i svaka grupa od dva znaka se pretvara u 11-bitni binarni niz. Na primjer, znakovi 'A' i 'B' su kodirani kao 10 i 11. Kombinacija 'AB' postaje 10 *45 + 11 = 461, što se zatim pretvara u binarni niz (0111001101)

3. Bajt

Kodiranje binarnih podataka uključujući ASCII tekst i druge binarne podatke tako što se svaki binarni broj pretvara u bajt (8 bita). Na početku se dodaje prefiks koji označava da je način kodiranja bajt 0100. Na primjer, riječ "Zdravo" bi se kodirala kao niz 8-bitnih binarnih nizova za svaki znak:

- Z – 01011010;
- D – 01000100;
- R – 01010010;
- A – 01000001;
- V – 01010110;
- O – 01001111;

01011010 01000100 01010010 01000001 01010110 01001111

4. Kanji

Ovaj metod omogućava kodiranje japanskih znakova pomoću ShiftJS kodne stanice. Radi se o specifičnom načinu kodiranja dizajniranom samo za efikasno rukovanje japanskim tekstom.

Svaki od ova četiri režima kodira tekst u niz bitova nula i jedinica, ali je razlika u metodi koju svaki niz koristi za pretvaranje teksta u bitove i svaka od metoda je optimizovana da podatke enkodira sa najkraćim mogućim nizom bitova. Iz tog razloga prvi korak u enkodiranju QR koda je analiza podataka kojom se utvrđuje da li će se tekst enkodirati numeričkom, alfanumeričkom, bajr ili Kanji metodom [16].

Korekcija greške

Korekcija greške predstavlja ključni korak u procesu generisanja QR koda i ona osigurava sigurnost podataka – da mogu biti pročitani čak i u slučaju djelimičnog oštećenja koda. Već je u radu napomenuto da se za ovaj korak koristi Reed-Solomonov algoritam za dodavanje redundantnih podataka koji omogućavaju ispravljanje grešaka.

Podaci koji će biti kodirani podijeljeni su u blokove. Veličina i broj blokova zavise o verziji i nivou korekcije grešaka. Veće verzije QR koda i viši nivoi korekcije grešaka zahtijevaju više blokova. Reed-Solomonov algoritam se primjenjuje na svaki blok podataka. Reed-Solomonovim kodiranjem se dodaje određeni broj redundantnih simbola za svaki blok podataka, u zavisnosti od nivoa. Blokovi podataka i njihovi odgovarajući bitovi za korekciju grešaka su međusobno isprepletani kako bi se povećala otpornost za oštećenja. Bitovi za korekciju grešaka se smještaju u QR kod matricu zajedno sa originalnim podacima. Nakon što se dodaju bitovi cijeli QR kod prolazi kroz još jednu provjeru kako bi se osigurala ispravnost kodiranih podataka.

Struktura konačne poruke

Na ovom koraku, unešeni podaci i ispravni kodovi za detekciju i korekciju greške koji su generisani u nekim od prethodnih koraka se organizuju i raspoređuju po odgovarajućem redosljedu. U ovom koraku se osigurava pravilno kodiranje i organizacija svih bitova podataka uključujući informacije o formatu, podatke i bitove za korekciju grešaka. Kada je riječ o velikim QR kodovima, podaci i ispravni kodovi se generišu u blokovima koji moraju međusobno biti prepleteni prema specifikaciji QR koda. Ovom strukturom omogućava se skenerima da precizno očitaju i dekodiraju QR kod.

Konačna poruka je struktuisana na sljedeći način:

- Prefiks – četvorobitni niz u zavisnosti od tipa poruke koja je kodirana (numerička, alfanumerička, bajt ili kajne),
- Bitovi koji označavaju broj znakova ili bajtova koji se kodiraju,
- Niz kodiranih podataka prema odabranom načinu kodiranja,

- Terminator – u slučaju da je završni binarni niz kraći od potrebne dužine (manji od 8 bitova),
- Bitovi Reed-Solomonovog kodiranja.

Podaci i bitovi za korekciju grešaka su međusobno isprepleteni kako bi se povećala otpornost na oštećenja. Ukoliko je konačna poruka na kraju kraća od predviđenog kapaciteta QR koda dodaju se PAD bitovi obično 11101100 i 00010001 naizmjenično, kako bi se popunila praznina do potpune veličine QR koda. Konačna poruka koja sadrži sve kodirane podatke i bitove za korekciju grešaka raspoređuje se u QR kod matricu [3], [16], [17].

Postavljanje modula

Postavljanje modula je proces u kojem se kodirani podaci i bitovi za korekciju grešaka fizički raspoređuju u matrici QR koda. Matrica QR koda sastoji se od modula (kvadratića) koji su organizovani u redovima i kolonama. Ovim procesom se osigurava da su svi elementi QR koda pravilno postavljeni i struktuirani omogućavajući skenerima tačno i nesmetano čitanje.

Maskiranje podataka

Maskiranjem podataka pomaže se u čitljivosti i pouzdanosti QR koda. Ovim korakom se izbjegavaju veliki blokovi kontinuiranih crnih ili bijelih modula koji mogu otežati pravilno skeniranje. Veliki blokovi istih boja (crnih ili bijelih modula) mogu zbuniti skenere i otežati pravilno skeniranje QR koda. Maskiranjem se mijenjaju određeni moduli radi boljeg kontrasta.

Unaprijed je definisano osam obrazaca maskiranja označenih od 0 do 7. Svaka maska se primjenjuje na module podataka i module za korekciju grešaka. Na primjer, maska 0 inverzno mijenja module gdje je pozicija (i+j) djeljiva sa 2, gdje su i i j redni i kolonski indeksi modula. Svaka maska se primjenjuje na cijeli QR kod i rezultat se procjenjuje prema definisanim kriterijumima. Maska koja rezultira najmanjim brojem konflikata i daje najbolji kontrast se bira kao konačna i primjenjuje na kodirane podatke.

Format i informacije o verziji

Posljednji korak u kodiranju QR koda je dodavanje informacija o formatu i u nekim slučajevima dodavanje piksela na određena područja koda koja su ostala nepopunjena u prethodnim koracima. Piskeli formata identifikuju nivo ispravke greške i maskni obrazac koji se koristi u ovom QR kodu. Pikseli verzije enkodiraju veličinu QR matrice i koriste se samo u većim QR kodovima. Formatne informacije sadrže nivo korekcije grešaka (L, M, Q, H) i obrazac maske koji je korišćen. Formatne informacije su kodirane u 15-bitnom nizu. Informacije o verziji sadrže broj verzije koda (npr. 1,2,3,....40) i potrebne su za verzije QR koda od 7 i više. Kodirane su u

18-bitnom nizu, a prvih 6 bitova predstavljaju broj verzije QR koda, dok su ostalih 12 BCH kodovi za korekciju grešaka. Ovi procesi omogućavaju ispravno identifikovanje korekcije greške, maske i verziju QR koda [17].

1.9 Primjer generisanja QR koda

Na sljedećem primjeru prikazan je algoritam koji generiše QR kod sa URL-om sajta Univerziteta Crne Gore: www.ucg.ac.me. Program je napisan u programskom jeziku Python.

```
import qrcode
import matplotlib.pyplot as plt

# Definisanje UR
url = "http://www.ucg.ac.me"

# Generisanje QR koda koristeći qrcode biblioteku
qr_code_qrcode = qrcode.make(url)

# Prikazivanje QR koda koristeći matplotlib
plt.imshow(qr_code_qrcode)
plt.axis('off')  # Isključivanje oznaka osa
plt.show()
```

Gore prikazani program generiše QR kod koji vodi na sajt Univerziteta Crne Gore i sačuvaće ga kao sliku.

Slika 12. Generisani QR kod

1.10 Algoritam dekodiranja QR koda

Algoritam dekodiranja QR koda uključuje nekoliko koraka koji su prikazani na slici 15. Prateći ove korake prepoznaju se i čitaju kodirani podaci da bi se na kraju dobio rezultat [17].

Slika 13. Algoritam dekodiranja QR koda

Od početka do kraja dešifrovanja, QR kod prolazi kroz osam, odnosno devet koraka u slučaju da se na šestom koraku detektuje greška.

Prepoznavanje modula

Prepoznavanje modula je prvi korak u algoritmu za dekodiranje QR koda. Ovaj korak uključuje identifikovanje strukture QR koda i njegovih ključnih elemenata da bi se postiglo pravilno očitavanje i dekodiranje podataka. Skenerom se slika QR kod, softver analizira sliku da bi identifikovao elemente QR koda. Prvo se prepoznaju pozicioni obrasci koji omogućavaju skeneru da odredi orijentaciju QR koda i njegove granice. Na osnovu obrazaca skener izračunava dimenzije i verziju koda. Prepoznaju se sinhronizacioni i obrasci poravnanja i na kraju svaki pojedinačni modul (kvadratić) unutar QR koda.

Ekstraktovanje informacija o formatu.

U koraku ekstraktovanja informacija o formatu, podaci o formatu QR koda bivaju dešifrovani iz odgovarajućih sekvenci koda. Ovi podaci o formatu uključuju i informacije o nivou korekcije grešaka i maskiranja. Nakon što se informacije o formatu ekstrakuju maskirni šabloni se primjenjuju na odgovarajuće djelove QR koda radi brisanja efekta maskiranja i omogućavanja daljeg dekodiranja podataka. Ukoliko je potrebno, ukoliko je došlo do greške bilo u spoljnjem ili unutrašnjem faktoru, na ovom koraku primjenjuje se i korekcija greške na informacijama o formatu radi obezbjeđivanja tačnih i pouzdanih informacija o formatu. Ova faza je, zapravo, ključna jer ona postavlja osnovne parametre za dalje dekodiranje podataka iz QR koda uključujući i nivo grešaka koje se mogu očekivati, te način na koji treba primjeniti maskiranje.

Određivanje informacija o verziji

U ovom koraku se provjerava da li je QR kod "opremljen" informacijama o verziji, odnosno da li ih sadrži. Ovi podaci su važni jer pružaju informacije o veličini i kapacitivnosti QR koda i na taj način omogućavaju dekodetru pravilno tumačenje strukture koda. Ukoliko su dostupne, ove informacije se dešifruju iz odgovarjaućih djelova QR koda. Nakon dešifrovanja, očitava se verzija QR koda, čime se omogućava dalje prilagođavanje procesa dekodiranja, a sve u skladu sa specifičnostima tog QR koda. Ovaj korak je jako bitan zbog toga što omogućava dekoderu da pravilno interpretira strukturu QR koda.

Oslobađanje maskiranja

U koraku oslobađanja maskiranja primjenjena maska se uklanja radi ispravnosti čitanja izvorno kodiranih podataka. Informacije o primjenjenoj maski se dobijaju iz formatnih informacija QR koda koje su već u prvom koraku dekodirane. Algoritam za oslobađanje maskiranja koristi isti

obrazac kao i za samo maskiranje, ali ovaj put u suprotnom smjeru. Moduli kodiranih podataka se analiziraju prema uzorku maske i svaki modul koji je bio inverzan se ponovo invertujeira da bi se vratio u svoj izvorni oblik. Npr. ukoliko je primjenjena maska 0. svaki modul na poziciji (i,j) gdje je (i + j) % 2 == 0, biće inverzno promijenjen.

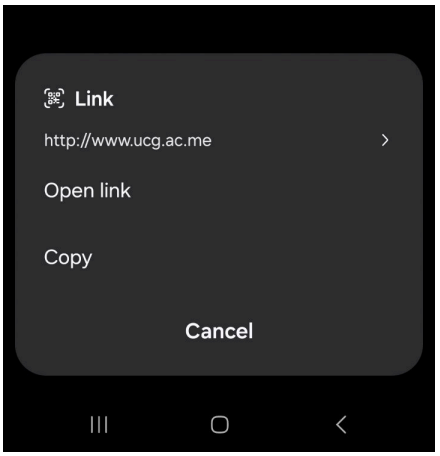
Obnavljanje podataka i kodova; detekcije greške

U koraku obnavljanja podataka i kodova detekcije greške svi moduli koji sadrže podatke i kodove za korekciju grešaka se identifikuju i izdvajaju. Ekstrakovani podaci se grupišu u blokove koji su međusobno isprepletani kako bi se povećala otpornost na oštećenja. Podaci i bitovi se dalje iz svakog bloka rekonstruišu u kodne riječi, a svaka kodna riječ sadrži niz bitova koji predstavljaju izvorne podatke i bitove za korekciju greške. Ovako rekonstruisane kodne riječi se pripremaju za provjeru grešaka koristeći Reed-Solomonov algoritam koji detektuje eventualne greške i određuje na kojim bitima su se desile greške i treba ih ispraviti. Ispravljeni podaci se rekonstruišu u izvorni oblik osiguravajući tačnost informacija.

Dekodiranje podataka

Nakon što su svi podaci obnovljeni i eventualne greške ispravljene, poruka je spremna za konačno dekodiranje. U ovom koraku dolazi do interpretacije binarnih podataka koji se rekonstruišu u izvorni tekst. Na osnovu prefiksa u podacima određuje se koji način je korišćen za kodiranje podataka. Nakon što je na osnovu prefiksa određen tip kodiranja podaci se prema odabranom načinu kodiranja dekodiraju:

- Ukoliko je tip kodiranja numerički grupe od tri cifre se dekodiraju u 10-bitne binarne nizove; dvije cifre u 7-bitne, a jedna cifra u 4-bitne binarne nizove;
- Ukoliko je tip kodiranja alfanumerički grupe od dva znaka se dekodiraju u 11-bitne binarne nizove;
- Svaki kodirani bajt se dekodira u odgovarajući ASCII znak;
- Svaki kanji znak se dekodira koristeći Shift JIS kodnu stranicu.



Slika 14.Dekodirana poruka

1.10.1 Napredni tipovi QR kodova

Sve veća popularnost QR kodova dodatno je potaknuta njihovim naprednim funkcionalnostima koje, uz osnovne mogućnosti, nude širok spektar dodatnih primjena.

- Dinamički QR kodovi

Ovi kodovi omogućavaju promjenu sadržaja QR koda nakon što je on već distribuiran, što znači da se informacije ili povezani resursi uz QR kod mogu ažurirati (npr. URL adresa). Ova funkcionalnost je korisna za različite marketinške kampanje, promocije, ili događaje na kojima se informacije mogu mijenjati tokom vremena i potrebno ih je ažurirati, a smanjuje i mogućnost greške. Dinamički QR kodovi sa sobom nose i veliku dozu rizika usljed podložnosti čestim promjenama.

- Višejezični QR kodovi

Ova vrsta QR kodova omogućava prilagodljivost teksta uslovima koji se koriste. Na primjer, QR kod može sadržati različite informacije ili povezane resurse u zavisnosti od lokacije, vremena ili demografskih specifikacija korisnika što im omogučuje personalizovaniji i korisnički okrenut sadržaj.

- QR kodovi sa višestrukim podacima

Tradiocionalni QR kodovi obično mogu sadržati samo ograničenu količinu podataka dok napredniji podržavaju veći kapacitet podataka čime se omogućuje dodavanje kompleksnih tipova podataka popout teksta, slika, zvuka ili videa.

- QR kodovi povezani sa analitičkim alatima

Omogućava praćenje broja skeniranja. Ova funkcionalnost je jako važna u različitim marketinškim i ostalim kampanjama, kada je važno pratiti broj korisnika do kojih je kampanja dospjela [3], [16], [17].

1.11 Integrisanost bezbjednosnih standarda u QR kod

QR kodovi sami po sebi ne pružaju sigurnosne mehanizme, ali postoje određeni standardi koji se mogu primjeniti, ili se primjenjuju, kako bi se bezbjednost podigla na veći nivo.

1. Korekcija greške – u radu je već navedeno da QR kodovi koriste Reed-Solomonov algoritam za korekciju grešaka čime se omogućava čitanje koda iako je djelimično oštećen,
2. Digitalni potpisi – ovi potpisi se mogu koristiti kako bi se osigurala autentičnost i integritet QR koda, odnosno da podaci nisu izmjenjeni, te da potiču od originalnog izvora,
3. Šifrovanje podataka – podaci unutar QR koda mogu biti šifrovani kako bi se zaštitili osjetljivi podaci od neželjenih pristupa; da bi se koristili šifrirani QR kodovi neophodno je da krajnji korisnik ima odgovarajući ključ za dešifrovanje podataka,
4. Verifikacija sadržaja – prije skeniranja QR koda korisnici mogu koristiti aplikacije koje provjeravaju URL-ove i ostale podatke koje QR kod može da sadrži, kako bi osigurali da će stići do pouzdanih adresa; ove aplikacije mogu provjeriti da li URL sadrži neku sigurnosnu prijetnju,
5. Dodatni slojevi autentifikacije – QR kodovi se mogu koristiti u kombinaciji sa drugim metodama autentifikacije poput lozinki ili biometrijskih podataka radi osiguranja autentičnosti pristupa,
6. Izbjegavanje javno dostupnih QR kodova – QR kodovi koji su javno dostupni mogu biti podložni manipulaciji pa se preporučuje korišćenje QR kodova unutar kontrolisanih okruženja gdje postoji manji rizik od neovlaštenih promjena,
7. Upotreba sigurnosnih aplikacija – korisnici mogu koristiti sigurnosne aplikacije koje analiziraju i ocjenjuju QR kodove prije nego ih skeniraju,
8. Edukacija o potencijalnim rizicima – Korisnici trebaju biti svjesni potencijalnih rizika povezanih sa skeniranjem QR kodova kao što su fišing napadi ili preusmjeravanje na zlonamjerne web stranice; u ovom dijelu je jako važna edukacija korisnika o sigurnosnim praksama [1], [3], [10].

2. Fišing napadi

Paralelno sa razvojem digitalnog svijeta i modernih tehnologija, razvijaju se i protivzakonite kriminalne aktivnosti na Internetu. Sajber kriminalci koriste digitalne resurse za ostvarivanje ilegalne dobiti, ciljajući pritom na pojedince, grupe ili korporacije, s namjerom da im nanesu štetu putem različitih oblika sajber napada. Cilj ilegalnih aktivnosti u digitalnom svijetu je prodiranje u privatnost kako bi se pristupilo osjetljivim informacijama, poput bankovnih računa i privatnih arhiva. Krađa identiteta, odnosno preuzimanje identiteta trećeg lica radi prisvajanja i korišćenja njegovih ličnih informacija, kao što su bankovni podaci, brojevi socijalnog osiguranja ili brojevi kreditnih kartica, predstavlja jedan od najvećih izazova i najopasnijih zločina koji prijete digitalnom svijetu.

Napadači su razvili svoje metode i tehnike za krađu informacija paralelno sa razvojem tehnologije, a veliki broj tih napada zasnovan je na socijalnom inženjeringu [11].

Jedan od napada koji omogućava krađu podataka meotodm socijalnog inženjeirnga jeste fišing (eng. phishing). Fišing je jedan od najvećih izazova sa kojima se susreću stručnjaci iz oblasti sajber bezbjednosti, ali i obični korisnici, jer mnogi korisnici na Internetu bivaju lako prevareni i postaju žrtve. Fišing je napad iz grupe socijalnog inženjeringa gdje napadač pokušava da zavara žrtvu kako bi pristupio njegovim osjetljivim informacijama slanjem poruka, putem elektronske pošte ili putem ostalih kanala za digitalnu komunikaciju. U posljednje vrijeme, QR kodovi se sve češće koriste u fišing napadima, tako da žrtva povjeruje poruci i otkrije osjetljive podatke napadaču, koji će te podatke kasnije zloupotrijebiti.

U fišing napadima, napadači koriste slabosti korisnika poput nepoznavanja ili neposjedovanja digitalne etike ili slabu obuku u kombinaciji sa ranjivostima radi postizanja vlastitih ciljeva. Istraživanja su pokazala da određene grupe osoba mogu biti podložnije različitim obmanama. Na primjer, osobe koje više slušaju autoritete nego druge imaju veće šanse da postanu žrtva napada poput Business Email Compromise koji se predstavljaju kao hitna pošta od finansijske institucije i zahtjeva neku hitnu akciju – najčešće informacije o računima u banci.

Još jedna od ljudskih slabosti koju napadači koriste u prevarama je pohlepa. Ovu ljudsku slabost napadači koriste prikazujući potencijalnim žrtvama velike popuste, besplatne poklon stvari, vaučere i slično.

Fišing napadi mogu dovesti ne samo do finansijskih gubitaka žrtve već i kroz druge ozbiljne posljedice poput gubitka reputacije ili u nekim širim slučajevima do kompromitovanja generalne bezbjednosti građana, [14].

2.1 Definicije fišinga

Stručnjaci i institucije koje se bave sajber bezbjednošću predložili su više definicija fišinga, tako da se nijedna od njih ne može smatrati "zvaničnom". Fišing se najjednostavnije može opisati i definisati kao proces obmanjivanja žrtve da preduzme određenu akciju koja je u interesu napadača, a na sopstvenu štetu. Studija *Merve et al.,2005* definiše fišing kao "fraudelantnu aktivnost koja uključuje stvaranje replike postojeće web stranice kako bi prevarila korisnika da dostavi lične, finansijske ili podatke lozinke.". Iako je od 2005. godine proširen spektar izvođenja fišing napada koncept i ideja su ostali isti.

Fišing napadi često nisu samo napadi na pojedinca, njegovu ličnost, privatnost i ugled, već mogu imati i dalekosežnije posljedice. Ljudi često na svojim mobilnim telefonima čuvaju poslovne podatke, uključujući poslovne komunikacione kanale (elektronska pošta ili aplikacije za interkompanijsku komunikaciju) i šifre zapisane u bilješkama na telefonu. Napadači su svjesni ovoga i razumiju da jedan upad u privatnost takve osobe može otvoriti pristup širem spektru informacija. Stoga, fišing predstavlja značajnu prijetnju ne samo za pojedince već i za organizacije, jer može dovesti do ozbiljnih sigurnosnih incidenata, gubitka povjerljivih informacija i finansijskih gubitaka. Prepoznavanje, edukacija i implementacija adekvatnih sigurnosnih mjera ključni su za zaštitu od ovakvih napada. Efikasna borba protiv fišinga zahtijeva koordinaciju između tehnoloških rješenja i svijesti korisnika, čime se može značajno smanjiti rizik od kompromitacije podataka.

2.2 QR kodovi kao alat za fišing napade

Iako QR kodovi nude brojne pogodnosti, oni se takođe koriste za napade. Napadači često ubacuju maliciozne kodne sekvence u QR kodove kako bi ostvarili svoje ciljeve. Jedan od glavnih nedostataka QR kodova je taj što su ih izumili ljudi, ali se njihovo generisanje i upotreba odvijaju automatizovano, bez mogućnosti da ljudsko oko razlikuje dobre od loših QR kodova. Prema ekspertima iz oblasti sajber bezbjednosti, napadi putem QR kodova su prilično efektivni, jer ljudsko oko i um nijesu sposobni da prepoznaju razlike među njima; za njihovo dešifrovanje potrebna je mašina.

Korisnici se često osjećaju komforno skenirajući slučajne QR kodove, jer su navikli da ih velike kompanije koriste u marketinške svrhe. Međutim, ovo može dovesti do ozbiljnih sigurnosnih rizika, jer zlonamjerni QR kodovi mogu preusmjeriti korisnike na fišing stranice ili navesti

korisnike na instaliranje zlonamjernog softvera na pametne uređaje. Ovi napadi mogu rezultirati krađom osjetljivih informacija i značajnim finansijskim gubicima. Stoga je važno da korisnici budu svjesni ovih rizika i preduzmu odgovarajuće mjere opreza prilikom skeniranja QR kodova, [13].

Koliko široke posljedice može imati neopreznost korisnika najbolje pokazuje podatak da su 2022. godine fišeri ukrali 12 miliona dolara u Sjedinjenim Američkim Državama dok su u Kini ukrali gotovo milion juana. U martu 2022. godine APWG (Anti Phishing Work Group – globalna organizacija koja se bavi borbom protiv fišinga) je zabilježio 384 291 napad, dok je u prvom kvartalu iste godine zabilježio preko milion pokušaja fišinga.

Kako bi fišing napad putem QR koda izgledao na konkretnom primjeru?

PRIMJER 1: Registraciona forma

Uzmimo primjer autobuskog stajališta, gdje napadač osmišljava plan da napravi sajt sličan zvaničnom sajtu za raspored polazaka autobusa, ali sa dodatnom registracionom formom koja zahtijeva podatke bankovne kartice korisnika, pod izgovorom da će im omogućiti plaćanje karticom. Link do takvog sajta se ubacuje u QR kod, koji se zatim lijepi na svim autobuskim stajalištima u gradu uz poruku "Od sada plaćanje platnim karticama".

Naivni korisnici, ne provjeravajući autentičnost informacije, svojim mobilnim telefonima skeniraju QR kod, što ih preusmjerava na lažni sajt. Taj sajt na prvi pogled izgleda uvjerljivo, prikazujući raspored vožnje autobusa, što korisniku stvara utisak legitimnosti. Korisnici se zatim registruju na sajtu, unoseći podatke svoje bankovne kartice, omogućavajući tako napadaču pristup njihovom bankovnom računu.

Ovaj primjer pokazuje kako se QR kodovi mogu zloupotrijebiti u fišing napadima, iskorištavajući povjerenje korisnika u poznate i svakodnevne situacije. Napadači koriste uvjerljive sajtove i društveni inženjering kako bi naveli korisnike da otkriju osjetljive informacije. Stoga je od ključne važnosti da korisnici uvijek provjeravaju autentičnost QR kodova i informacija prije nego što im povjere svoje osjetljive podatke.

PRIMJER 2: Preuzimanje aplikacije

Slična situacija, ali još lakša za napadača, bila bi sa aplikacijom. Na autobuskom stajalištu pojavljuje se "reklama" koja sadrži tekst "Nova aplikacija sa novim redovima vožnje autobusa! SKENIRAJTE QR KOD I PREUZMITE APLIKACIJU". Skeniranjem QR koda, žrtva će biti

preusmjerena na URL link gdje se nalazi aplikacija za preuzimanje. Nakon što žrtva preuzme aplikaciju, napadač će imati pristup njenom uređaju, uključujući bankovne aplikacije, e-mailove, poslovne naloge, kao i privatne podatke poput društvenih mreža, galerije fotografija i slično, čime može ucjenjivati žrtvu.

Naivnom korisniku ova "reklama" neće biti ništa sumnjiva. Skeniraće QR kod, otvoriti link, preuzeti aplikaciju i tako omogućiti napadaču pristup svom telefonu.

Ovaj primjer dodatno ilustruje kako napadači koriste QR kodove za fišing napade i eksploataciju korisnika, iskorištavajući njihovu naivnost i povjerenje. Važno je da korisnici budu oprezni i skeptični prema ovakvim reklamama, te da provjeravaju autentičnost QR kodova prije nego što ih skeniraju i instaliraju aplikacije.

Preporuke za izbjegavanje fišing napada putem QR kodova

Kako bi se smanjila opasnost od fišing napada putem QR kodova, korisnici trebaju slijediti određene sigurnosne mjere. Na primjeru autobuskog stajališta, gdje napadač postavlja lažne QR kodove moguće je preduzeti sljedeće mjere predostrožnosti:

Primjer 1: Autobusko stajalište

1. **Provjera informacija**:
    - **Preporuka**: Prije skeniranja QR koda, provjeravanje zvaničnih izvora poput zvaničnog sajta Glavnog grada (u gore navedenom slučaju), ili sajta pružaoca usluga. Na tim sajtovima bi trebale postojati informacije o bilo kakvim novostima ili promjenama u uslugama.
2. **Provjera teksta pored QR koda**:
    - **Preporuka**: Napadači često prave greške u pisanju ili koriste nekvalitetan jezik i iz tog razloga bi bilo preporučljivo pročitati detaljno tekst koji se nalazi pored QR koda.
    - **Razlog**: Greške u tekstu mogu biti znak upozorenja da QR kod nije legitiman. **Provjera sadržaja sajta**
    - **Preporuka**: Legitiman sajt će imati profesionalan izgled i funkcionalnost. Ukoliko postoji bilo kakva, i najmanja greška na sajtu, gramatičke, pravopisne ili neke druge prirode postoji realna mogućnst da sajt nije vjerodostojan.
    - **Razlog**: Neuredni ili nepouzdani sajtovi često signalizuju pokušaj prevare.
3. **Nepovjerljivost prema hitnim zahtjevima**:

- **Preporuka**: Fišeri često pozivaju na hitne akcije kako bi korisnicima ostavili što manje vremena za razmišljanje o potencijalnoj prevari. Ukoliko poziva na hitnu reakciju, vjerovatno se radi o prevari.

4. **Dvostruka provjera prije unosa podataka**:
    - **Preporuka**: Prije nego što unesete podatke platne kartice, dvostruko provjerite sa zvaničnim izvorima kao što su banka ili pružalac usluga.
    - **Razlog**: Osjetljivi podaci trebaju biti unijeti samo na provjerene i sigurne sajtove.

PRIMJER 2 – Preuzimanje aplikacije

Slična situacija može se dogoditi i sa preuzimanjem aplikacija. Napadači mogu postaviti lažne reklame sa QR kodovima koji vode na zlonamjerne aplikacije. Da bi se zaštitili, korisnici trebaju da poštuju određena pravila:

1. **Provjera zvaničnih izvora aplikacija**:
    - **Preporuka**: Preuzimajte aplikacije isključivo iz zvaničnih prodavnica aplikacija kao što su Google Play Store ili Apple App Store.
    - **Razlog**: Zvanične prodavnice aplikacija imaju stroge sigurnosne provjere koje smanjuju rizik od prezimanja zlonamjernih aplikacija.
2. **Provjera ocjena i recenzija**:
    - **Preporuka**: Provjerite ocjene i recenzije aplikacije prije preuzimanja. Negativne recenzije ili mali broj preuzimanja mogu biti znak upozorenja.
    - **Razlog**: Korisničke recenzije mogu pružiti dodatne informacije o sigurnosti i funkcionalnosti aplikacije.
3. **Provjera dozvola aplikacije**:
    - **Preporuka**: Pažljivo pregledajte dozvole koje aplikacija traži prije instalacije. Ako aplikacija traži previše dozvola koje nisu u skladu sa njenom funkcionalnošću, to može biti znak opasnosti.
    - **Razlog**: Zlonamjerne aplikacije često traže nepotrebne dozvole kako bi dobile pristup osjetljivim podacima.

2.4 Vizuelna analiza QR kodova – prepoznavanje prijetnji

Mijenjajući ulazne parametre i podatke poput dizajna, funkcionalnih komponenti i logotipova značajno se mijenja i izgled samog QR koda.

Uzmimo za primjer QR kod koji vodi na URL adresu Univerziteta Crne Gore.

Slika 15. QR kod u originalnom obliku, sa malim izmjenama i sa velikim izmjenama

Na slici 15. prikazan je QR kod u kome je kodirana URL adresa „*ucg.ac.me*". Na drugom QR kodu je adresa "*ucgggggggggg.ac.me*" dok je treći potpuno izmjenjen i njime je kodirano "*ucccccccccccccccccccccccccccccccccccccccccccccgggggggggggggggggggggg.ac.me,,*. I dok je potpuno uočljivo da posljednji QR kod ne izgleda uobičajeno i da se radi o potencijalnoj prevari, gotovo je nemoguće otkriti ''golim okom'' da postoji razlika između prva dva. Pomenuta razlika jasno je uočljiva skeniranjem QR koda. Na slici 16. prikazani su izlazni podaci skeniranja sva tri QR koda.

Slika 16. Rezultati skeniranja QR kodova sa slike 16.

U ovoj fazi već je jasno uočljivo koji skenirani QR kod nosi potencijalnu opasnost.

Danas su, pogotovo u marketinške svrhe sve popularniji QR kodovi koji sadrže logo kompanije u sredini. Upravo je ovaj tip QR koda napadači vide idealnim svojim sredstvom. Ne postoji provjera vjerodostojnosti logotipa koji se nalazi u sredini QR koda sa informacijom koja je šifrirana unutar njega.

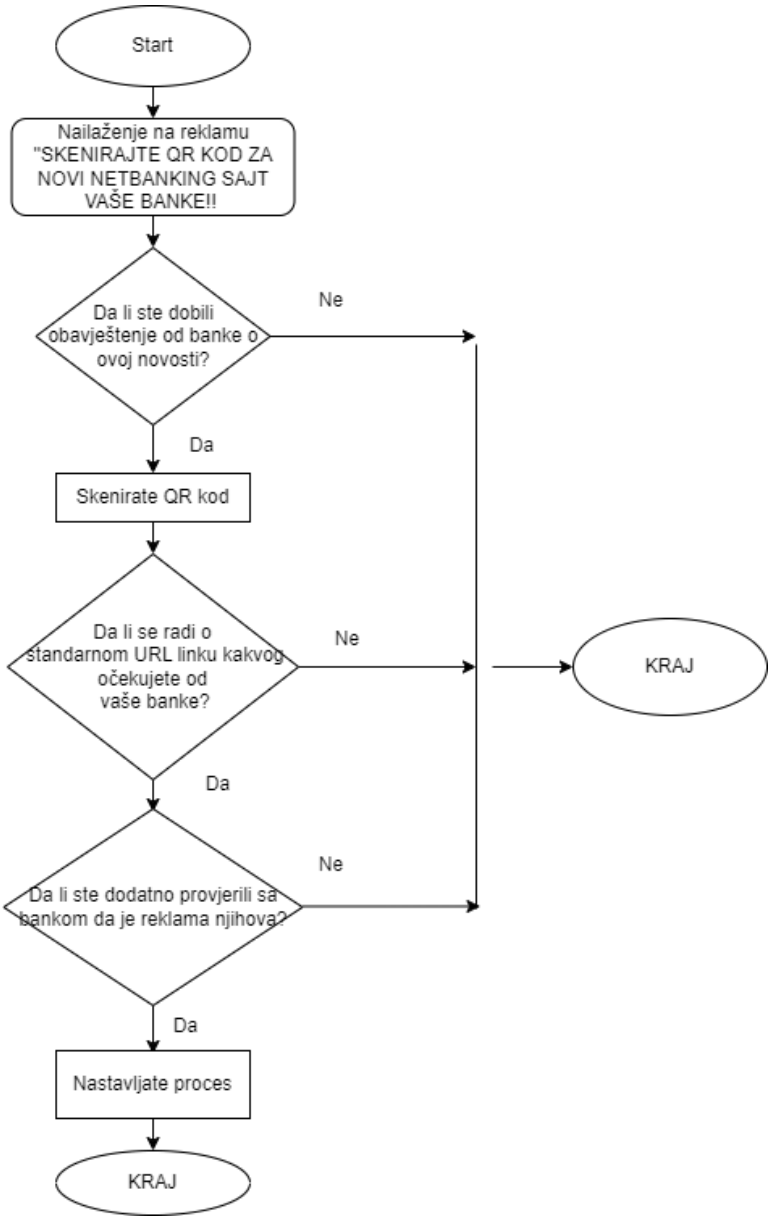
Uzmimo ponovo primjer QR koda koji vodi na link ucg.ac.me a u sredinu stavimo random logotip, recimo znak "😊".

Slika 17. QR kod sa lažnim logotipom

Na slici 17. prikazan je QR kod u kome je kodiran URL link Univerziteta Crne Gore sa lažnim logotipom u sredini. Na ovaj način bi zlonamjerni napadači mogli da iskoriste bilo koji logotip, natjeraju naivne korisnike da povjeruju da će skeniranjem QR koda otvoriti stranicu logotipa koji su prikazali i natjerati ih u „zamku“.

2.5 Algoritam prepoznavanja fišing QR koda

Gotovo svakim QR kodom koji skenira krajnji korisnik nosi rizik da je možda skenirao QR kod sa malicioznom sekvencom koda koja će otvoriti neki fišing sajt. U svakom slučaju korisnik treba se voditi algoritmom odlučivanja prikazanim na slici 18. [6].



Slika 18. Algoritam "sigurnog" ponašanja pri skeniranju QR koda

2.5.1 Automatizovana skripta za prepoznavanje sigurnog QR koda

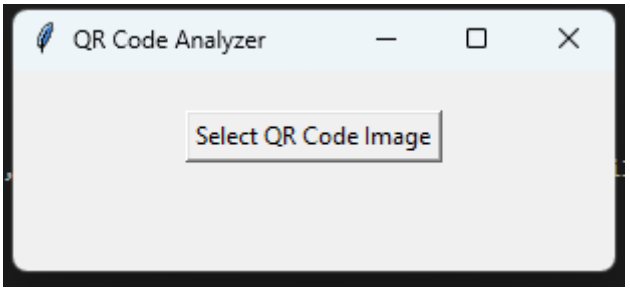
Sigurno skeniranje QR koda moguće je postići upotrebom dodatnih softverskih alata za prepoznavanje potencijalnog fišinga koji se krije iza QR koda, [8]. U okviru rada odrađena je i automatizovana skripta koja analizira QR kod, dešifruje ga i analizira URL kod.
Skripta je napisana u programskom jeziku Python i provjerava da li URL koji je integrisan u QR kod može biti potencijalni fišing integracijom sa bazom podataka poznatih fišing URL-ova.

Kako bi se postigli željeni rezultati, upotrijebljeno je nekoliko ključnih tehnologija i to:

1. OpenCV i Pyzbar – Pythonove biblioteke za obradu slika i dekodiranje QR kodova,

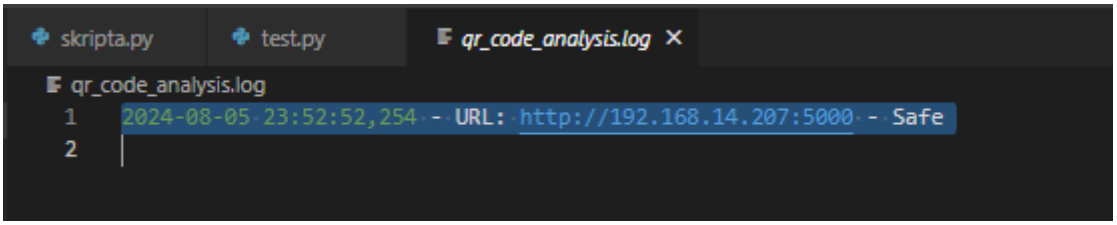
2. Requests – Za slanje HTTP zahtjeva i provjeru URL-a integracijom sa bazom podataka poznatih fišing sajtova,
3. Pandas – za organizaciju i generisanje izvještaja u .csv formatu,
4. Tkinter – za razvoj GUI-a.

Pokretanjem skripte otvoriće se prozor za odrabir QR koda.

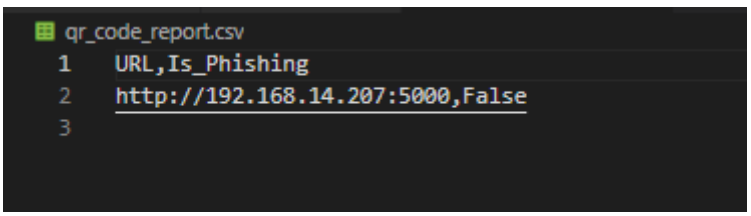


Slika 19. Korisnički interfejs programa za prepoznavanje fišing QR koda

Nakon što se programu „preda“ kod na analizu, rezultati analize se čuvaju u .log fajlu za kasniju analizu, dok se rezultati te analize čuvaju i prikazuju u .csv fajlu radi lakšeg pregledanja i izvještavanja.



Slika 20. Log fajl koji služi za analizu rezultata



Slika 21. Rezultat analize

Kako bi kod mogao biti iskorišćen za dalja istraživanja na temu, ostavljen je kao dio rada. [12]

```
import requests
import cv2
import logging
import tkinter as tk
from tkinter import filedialog, messagebox
from pyzbar.pyzbar import decode
import pandas as pd


# Konfiguracija logovanja
logging.basicConfig(filename='qr_code_analysis.log',      level=logging.INFO,
format='%(asctime)s - %(message)s')


# Funkcija za dekodiranje QR koda iz slike
def decode_qr_code(image_path):
    image = cv2.imread(image_path)
    if image is None:
        raise FileNotFoundError(f"Canot open/read file: {image_path}")
    qr_codes = decode(image)
      urls  =  [qr_code.data.decode('utf-8')  for  qr_code  in  qr_codes  if
qr_code.type == 'QRCODE']
    return urls


# Funkcija za provjeru da li je URL potencijalno fišing
def check_url(url):
```

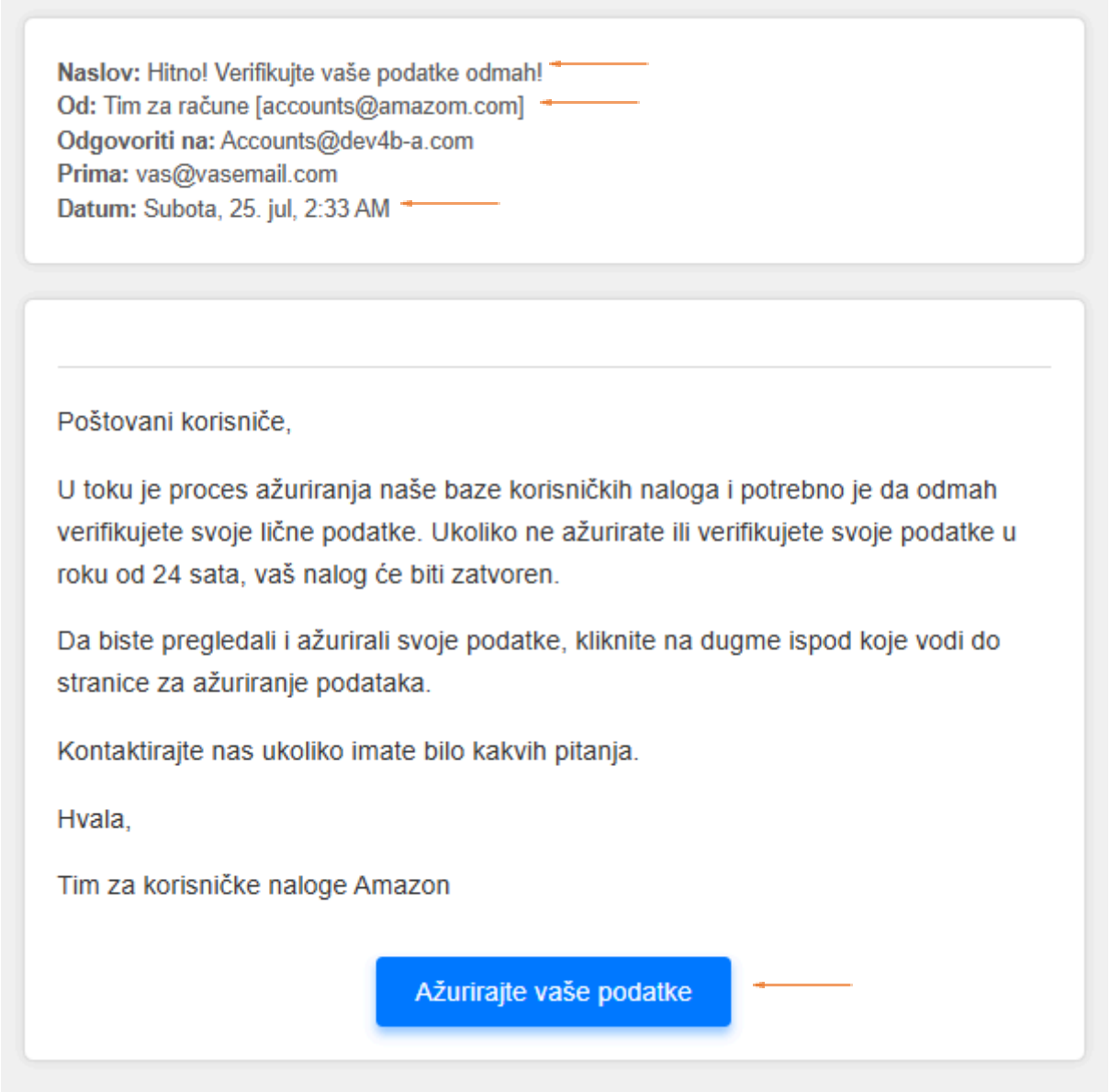
```
# Funkcija za generisanje izveštaja
def generate_report(results, report_path):
    df = pd.DataFrame(results)
    df.to_csv(report_path, index=False)
    print(f"Report generated: {report_path}")

# GUI za biranje fajla i pokretanje analize
def run_gui():
    def select_file():
        file_path = filedialog.askopenfilename()
        if file_path:
            try:
                results = analyze_qr_code(file_path)
                generate_report(results, 'qr_code_report.csv')
                    messagebox.showinfo("Success", "Analysis complete. Report
generated as 'qr_code_report.csv'.")
            except Exception as e:
                messagebox.showerror("Error", str(e))

    root = tk.Tk()
    root.title("QR Code Analyzer")
    root.geometry("300x100")

        btn_select_file = tk.Button(root, text="Select QR Code Image",
```

2.6 Primjer fišing napada izvedenog putem elektronske pošte



Slika 22. Fišing napad izveden putem elektronske pošte

Na slici 22. prikazan je primjer fišing napada izvedem preko elektronske pošte. Strelicama i crvenim slovima označeni su ključni faktori za prepoznavanje fišing mejla.

1. Poziv na hitnu akciju - napadači često koriste ovu vrstu manipulacije kako bi skratili vrijeme žrtvi i šanse da ne nasjedne na prevaru.

2. Email adresa koja jako podsjeća na pravu sa samo jednim slovom koje pravi razliku,
3. Vrijeme – hakeri rade često kasno u noć i tada napadaju – ovo može biti ključni znak za prepoznavanje fišing napada,
4. Poziv na akciju – ostavljanje podataka.

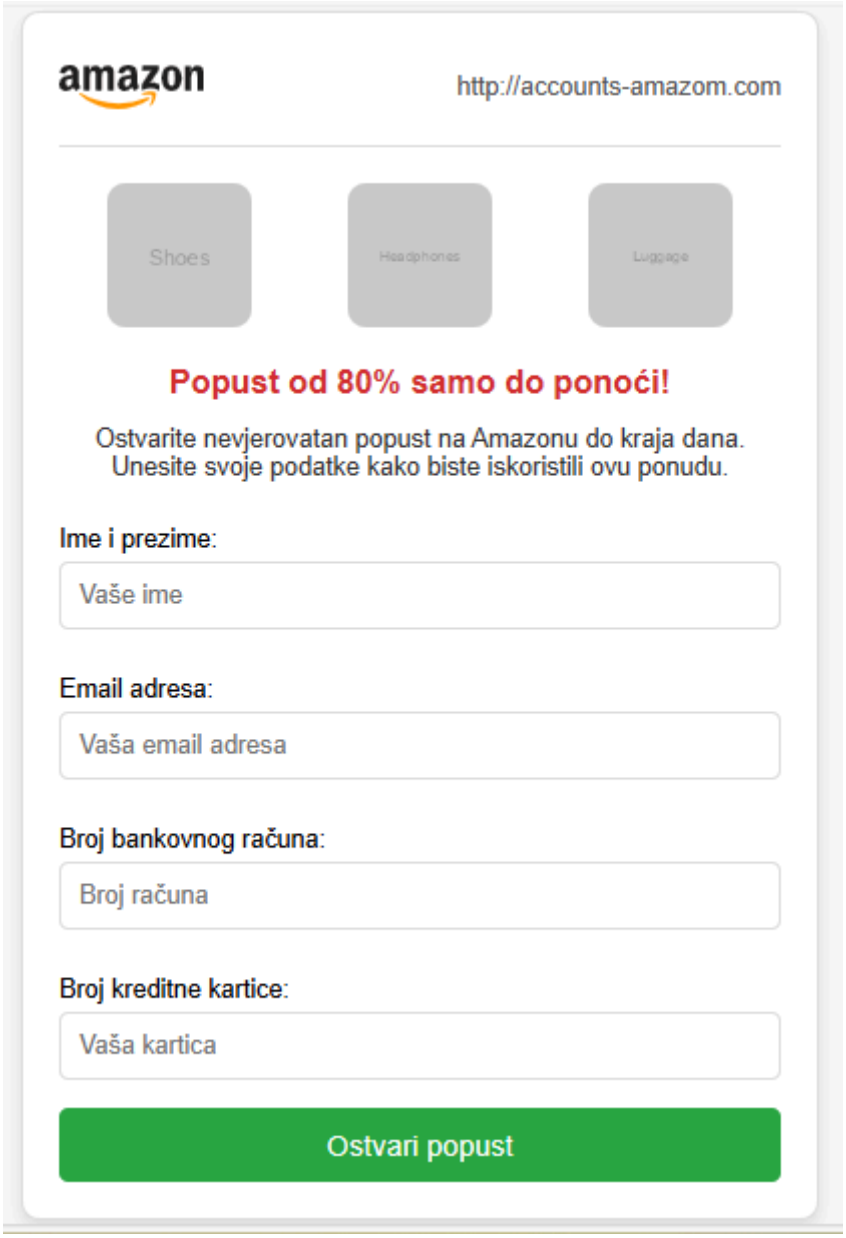
Dakle, ključni faktor u provjeri fišing napada jeste provjera i nepreduzimanje nikakve akcije ukoliko postoji i najmanja sumnja u vjerodostojnost sadržaja mejla.

Sličan način provjere bio bi i u slučaju fišing napada izvedenog putem QR koda.

Uzmimo sljedeći primjer:

Na društvenim mrežama i nekoliko lokacija u gradu osvanuo je sponzorisani oglas koji kaže da je na svjetski poznatom brendu online kupovine *Amazonu* veliki popust od čak 80% i da isti traje samo do ponoći. Da bi se ostvario popust potrebno je skenirati QR kod.

Slika 23. Primjer fišing reklame



Slika 24. FIšing napad izveden putem QR koda - primjer: online prodavnica

Na slici broj 24. prikazan je primjer pažljivo odrađenog fišing napada. Žrtva je preusmjerena na stranicu koja zaista liči na originalnu stranicu – upotrijebljen je originalni *Amazon* logo kao i simbolične slike prodaje. U ovom slučaju žrtva "mora" provjeriti URL adresu. Na URL adresi je promijenjeno jedno slovo u odnosu na originalno – umjesto amazo**n** piše amazo**m**. I upravo su razlike takve prirode najčešće u fišing napadima u odnosu na originalne URL adrese.

Ukoliko korisnik ne bi bio obazriv vrlo lako bi upao u zamku: na login stranici unio bi svoje podatke, napravio neku narudžbu koja bi bila lažna, napravio uplatu i ostavio podatke svoje

platne kartice i na taj način dao mogućnost napadaču da raspolaže sredstvima sa njegovog bankovnog računa.

2.7 Izvođenje ostalih hakerskih napada posredstvom QR kodova

Fišing napadi predstavljaju idealnu polaznu tačku za mnoge druge hakerske napade, jer se oslanjaju na tehnike socijalnog inženjeringa koje manipulišu korisnicima kako bi otkrili osjetljive informacije. QR kodovi, kao sredstvo koje ne pruža visok nivo zaštite neupućenim korisnicima, postali su popularan alat među napadačima. Kombinacija jednostavnosti korišćenja i nedostatka svijesti o potencijalnim rizicima čini QR kodove izuzetno efikasnim u izvođenju različitih vrsta cyber napada [15], [24].

Kada korisnici skeniraju QR kodove, oni ne vide stvarne URL adrese ili sadržaj koji kod krije, što omogućava napadačima da lako sakriju zlonamjerne namjere. Ovo ih čini idealnim za distribuciju zlonamjernog softvera, krađu identiteta, preusmjeravanje na lažne web stranice i mnoge druge oblike sajber kriminala. Napadači koriste socijalni inženjering kako bi stvorili osjećaj hitnosti ili legitimnosti, što korisnike navodi na brzo djelovanje bez odgovarajuće provjere.

Ovaj pristup omogućava napadačima da iniciraju napade poput instaliranja zlonamjernih aplikacija, preuzimanja kontrole nad uređajima korisnika ili pristupa njihovim osjetljivim podacima. U kombinaciji sa sofisticiranim tehnikama socijalnog inženjeringa, QR kodovi postaju moćan alat u arsenalu sajber kriminalaca.

2.7.1 Malware napad izveden putem QR koda

Eksponencijalnim rastom popularnosti QR kodova dešavaju se i sve češći malware napadi putem istih. Napadači mogu iskoristiti QR kodove za preusmjeravanje korisnika na zlonamjerne web stranice koje navode da preuzimaju malware na njihove uređaje.

Mehanizam Napada

Zlonamjerni URL-ovi: QR kodovi mogu sadržati URL koji preusmjerava korisnika/cu na zlonamjernu web stranicu. Ove stranice mogu izgledati legitimno i često ih je jako teško razlikovati on onih legitimnih jer su dizajnirane da preuzmu malware na uređaj korisnika.

Automatsko preuzimanje: Kada korisnik skenira QR kod i otvori zlonamjerni URL, može doći do toga da automatski započne preuzimanje malware-a na uređaj kojim je skeniran QR kod. Ovo

može biti u obliku aplikacija, datoteka ili skripti koje iskorišćavaju ranjivosti u operativnom sistemu ili aplikacijama.

Otmica podataka: Nakon preuzimanja, malware može pristupiti osjetljivim podacima na uređaju, kao što su kontakti, fotografije, SMS poruke i bankovne informacije.

2.7.2 Pharming napad izveden posredstvom QR koda

Napadač može manipulisati QR kodom na taj način da korisnika preusmjeri na neku lažnu web stranicu koja izgledom podsjeća na originalnu, a na kojoj se prodaje neka legitimna usluga ili proizvod. Na primjer, nakon što skenira QR kod korisnik može biti prevaren da je otvorio web stranicu za prijavu na svoj bankovni račun ali zapravo svoje podatke preusmjerava na lažnu stranicu koja krade korisnička imena i lozinke. Dakle, pharming napadi su sofisticiranija verzija napada u kojoj dolazi do modifikovanja DNS-a, a kojoj lako mogu podlijeći svi korisnici.

Mehanizam Napada

- **Preusmjeravanje DNS-a:** QR kod može sadržati URL koji koristi preusmjeravanje DNS-a kako bi korisnik bio usmjeren na lažnu web stranicu koja izgleda identično kao legitimna.
- **Krađa Podataka:** Korisnici unose svoje podatke na lažnu web stranicu misleći da je legitimna. Ovi podaci se zatim skupljaju i koriste za zlonamjerne aktivnosti.

2.7.3 Socijalni inženjering i QR kodovi

QR kod može biti dio neke kampanje socijalnog inženjeringa koja korisnicima na prvi pogled obećava nešto privlačno ili hitno (npr. neku nagradu ili popust u prodajnim objektima) a zapravo "žrtvu" vodi do napada ili krađe podataka.

Skeniranje QR kodova je postalo ranjivo zato što ljudsko oko ne može da razlikuje zlonamjerni QR kod od onog koji to nije. Opasnost koja se krije iza QR kodova ne samo da može imati uticaj na pojedinca već i na čitave organizacije. Iz tog razloga je jako važno govoriti o ovoj temi što je moguće više i šire. [20]

Mehanizam Napada

- **Manipulacija:** Napadači koriste QR kodove u e-mailovima, porukama ili na javnim mjestima, tvrdeći da QR kod vodi do korisnih informacija ili ponuda.
- **Lažni zahtjevi:** Korisnici su navedeni da skeniraju QR kodove koji vode do fišhing stranica, lažnih aplikacija za preuzimanje ili formi za unos ličnih podataka.

Rezultat

Rezultati svih napada su uglavnom slični, dolazi do krađe informacija jer korisnici nesvjesno mogu otkriti svoje privatne podatke, podatke o računima u banci itd. Korisnik može izgubiti pristup svom uređaju instalacijom malware softvera ili izgubiti pristup nalozima na Internetu te doživjeti finansijske i druge gubitke.

3. Uticaj (ne)poznavanja bezbjednosnih standarda na fišing napade izvedene putem QR kodova

Bezbjednost na Internetu postala je jedna od ključnih tema u digitalnom svijetu i društvu, a kako proces digitalizacije rapidno raste, rastu i savremena digitalna rješenja u svakodnevnom društvu poput QR kodova koji su efikasno sredstvo za brzo povezivanje sa različitim informacijama. Ipak, sa porastom popularnosti QR kodova porasla je zabrinutost jer se sve više putem QR kodova izvode fišing napadi. Oni predstavljaju ozbiljnu prijetnju korisnicima Internet servisa, a najveći uticaj mogu imati po korisnike čiji nivo poznavanja bezbjednosnih standarda ne zadovoljava potrebe sigurnosti.

Iz tog razloga, u okviru ovog rada sprovedena je anketa nad 141 ispitanika/ca koji su dali odgovore u vezi sa poznavanjem sigurnosnih standarda povezanih sa QR kodovima. Cilj ovog anketnog istraživanja jeste da kroz analizu rezultata razumije nivo svijesti i znanja korisnika o bezbjednosnim rizicima povezanim sa korišćenjem QR kodova kao i identifikacija ključnih faktora koji utiču na njihovu podložnost fišing napadima.

3.1 Aspekti anketnog istraživanja

Anketno istraživanje u sklopu rada temelji se na metodološkim smjernicama anketa u društvenim naukama a prije svega na validaciji i temeljnoj analizi podataka kako bi se osigurali pouzdani i reprezentativni rezultati. Tokom osmišljavanja ankete korišćene su ključne dimenzije kvaliteta podataka, kao što su relevantnost konceptualne mape i vjernost podataka čime se osigurava postizanje željenih rezultata odnosno uvid u bezbjednosne rizike koje nosi skeniranje QR kodova za potrebe istraživanja, a ispitanicima se osigurava jasno razumijevanje postavljenih pitanja. U tom smislu, analizirane su demografske karakteristike ispitanika kao potencijalni indikatori ranjivih grupa, čime se omogućava bolje razumijevanje uzoraka ponašanja i svijesti o sigurnosnim rizicima skeniranja QR kodova [25], [26].

Anketa je sprovedena elektronskim putem, putem Google forme, bila je u potpunosti anonimna.

Anketa je podijeljena u četiri sekcije, a u svakoj od njih ispitanici/ce su odgovarali na pitanja iz različitih oblasti koja su manje ili više povezana jedna s drugom.

Prva oblast obuhvatila je opšte informacije o ispitanicima/cama, koje su u svrhu istraživanja pomogle da se stvori slika o polu, starosti, stepenu obrazovanja, kao i oblasti rada/nauke iz koje ispitanici/ce dolaze. Druga oblast ispitivala je opštu informisanost ispitanika/ca o QR kodovima, da li ih koriste i da li su upoznati sa pojmom. Treća oblast ispitivala je anketirane učesnike/ce o opštoj informisanosti o bezbjednosti i rizicima koji postoje u sajber prostoru, te nivou poznavanja pojma sajber bezbjednosti i fišing napada. U posljednjoj, odnosno četvrtoj oblasti, provjeravao se nivo svjesnosti o opasnostima koje dolaze i kriju se iza QR kodova.

U narednim tabelama i grafikonima biće prikazani rezultati ankete na osnovu datih odgovora. Aknetna pitanja navedena su u Dodatku 1.

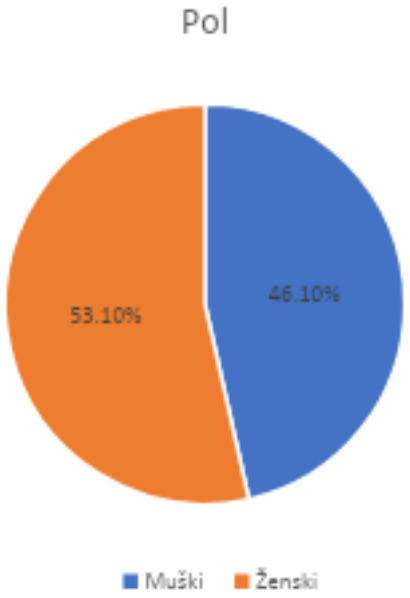
3.2 Demografska analiza ispitanika

U prvom dijelu rezultata ankete biće prikazana demografska analiza anketiranih učesnika.**Pol učesnika/ca ankete**

Što se tiče rodne zastupljenosti, imamo gotovo jednaku raspodelu između muškaraca i žena, sa blagom prednošću ženskog pola. Ova ravnoteža omogućava reprezentativniji uzorak za analizu.

Tabela 3. Prikaz odgovora o polu učesnika ankete na uzorku od 141 odgovora.

Pol	
Muškarci	Žene
65	76



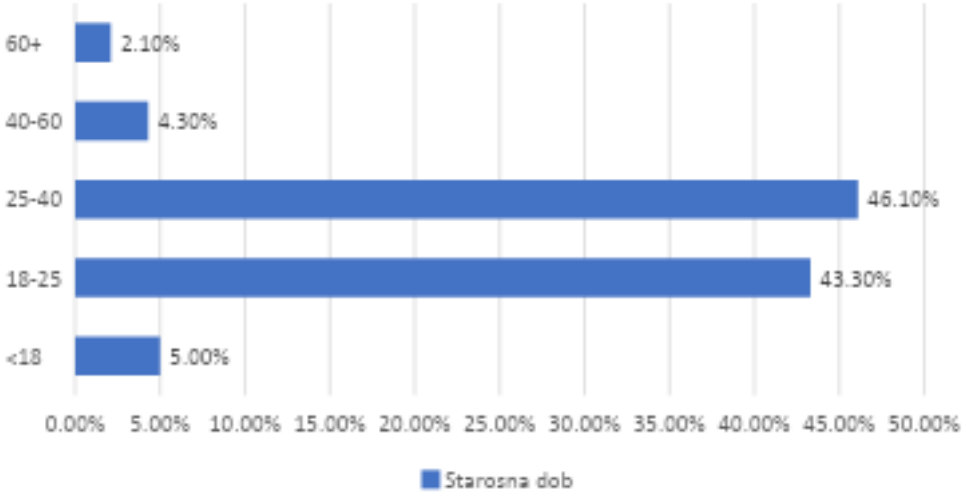
Grafik 1. Raspodjela učesnika/ca prema polu

Starosna struktura

Ispitanici su razvrstani u različite starosne grupe. Najveći broj ispitanika pripada grupi od 25-40 godina, što ukazuje na to da su odrasle osobe srednjih godina najzastupljenije u uzorku.

Tabela 4. Prikaz odgovora na pitanje o godinama u anketi

Starosna dob				
<18	18-25	25-40	40-60	60>
7	61	65	6	3



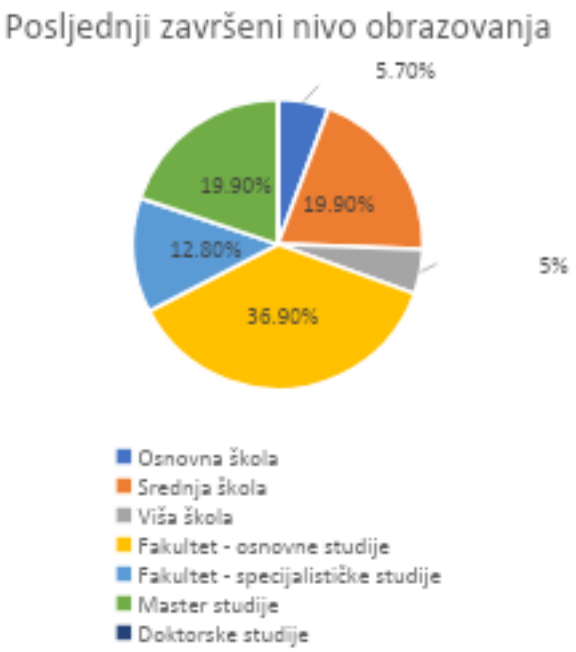
Grafik 2. Procentualni prikaz starosti učesnika/ca ankete.

Posljednji završeni nivo obrazovanja

Većina ispitanika ima završene osnovne studije (fakultet), dok je značajan broj njih završio i master studije. Takođe, imamo i određeni broj ispitanika sa srednjom školom i specijalističkim studijama. Ovi podaci nam ukazuju da su ispitanici generalno visoko obrazovani.

Tabela 5. Posljednji završeni nivo obrazovanja učesnika/ca u anketi

Posljednji završeni nivo obrazovanja						
Osnovna škola	Srednja škola	Fakultet – osnovne studije	Viša škola	Fakultet – specijalističke studije	Master studije	Doktorske studije
8	28	52	7	18	28	0



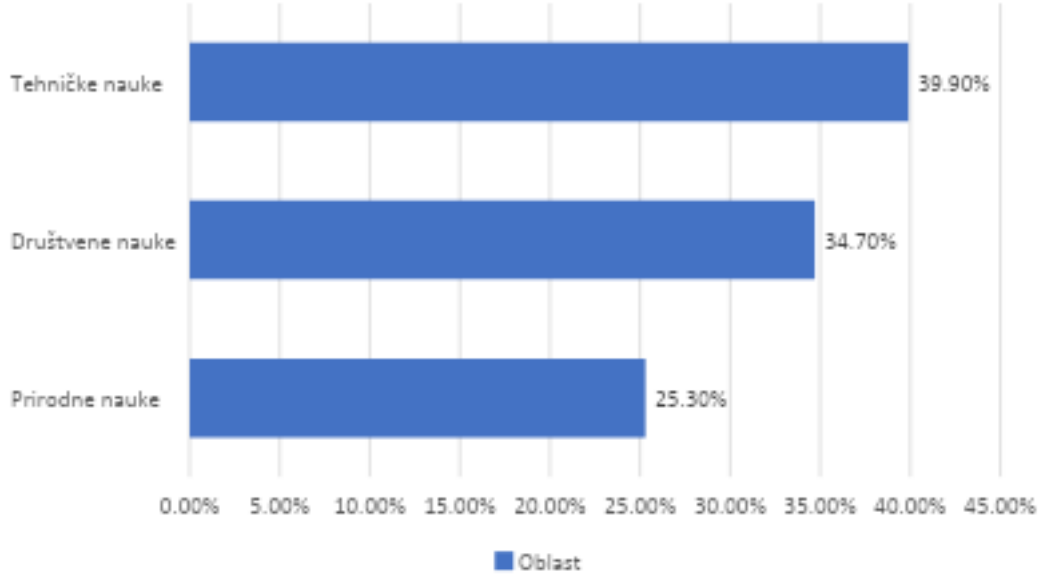
Grafik 3. Posljednji završeni stepen obrazovanja učesnika/ca

Oblast rada (zanimanje)

Anketirani učesnici/ce su odgovorili na pitanje o oblasti zanimanja. Na ovo pitanje 138 učesnika/ca je dalo odgovor. Pitanje je koncipirano na način da se izdvoje prirodne nauke, društvene nauke te tehničke nauke.

Tabela 6. Oblast rada ispitanika/ca ankete

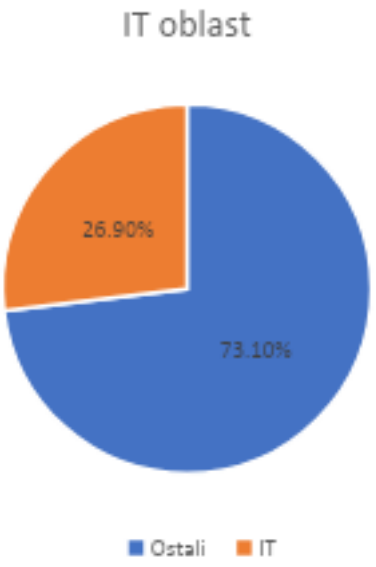
Oblast rada – zanimanja		
Prirodne nauke	Društvene nauke	Tehničke nauke
35	48	55



Grafik 4. Oblast rada/zanimanja

Učesnici/ce ankete iz oblasti informacionih tehnologija

Od 39.90% učesnika/ca ankete koji su odgovorili da dolaze iz sfere tehničkih nauka, njih 35 ukupno odnosno ukupno 35.4% dolazi iz oblasti informacionih tehnologija. Na ukupnom uzorku ankete to je nešto manje od 27%.



Grafik 5. Udio IT stručnjaka među učesnicima/učesnicama ankete

Ova početna demografska analiza pruža dobar uvid u strukturu ispitanika, što je ključno za dalju analizu njihovih odgovora i stavova prema QR kodovima i bezbjednosnim mjerama koje preduzimaju.

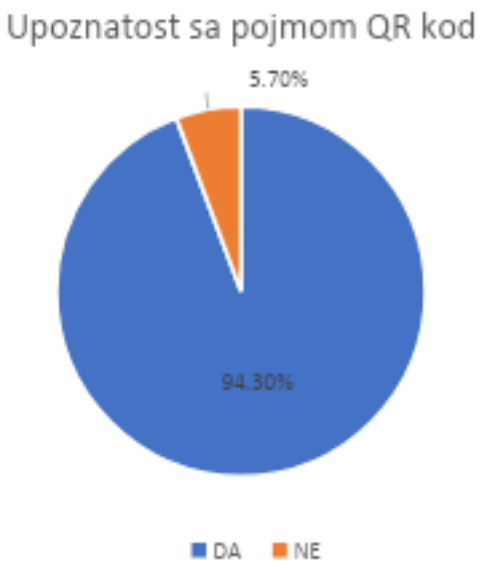
3.3 Opšte poznavanje QR kodova

Drugi dio ankete posvećen je opštem poznavanju pojma QR koda i na njemu su bila sljedeća pitanja:

1. Da li znate šta su QR kodovi?
2. Da li ste u posljednjih 10 dana skenirali neki QR kod?

Da li znate šta su QR kodovi?

Od 141 učesnika/ce koji su dali odgovor na ovo pitanje 133 je odgovorilo „Da“ dok je „Ne“ odgovorilo 8 učesnika/ca. Odgovori na ovo pitanje ukazuju na generalnu poznatost sa postojanjem i funkcijom QR kodova.



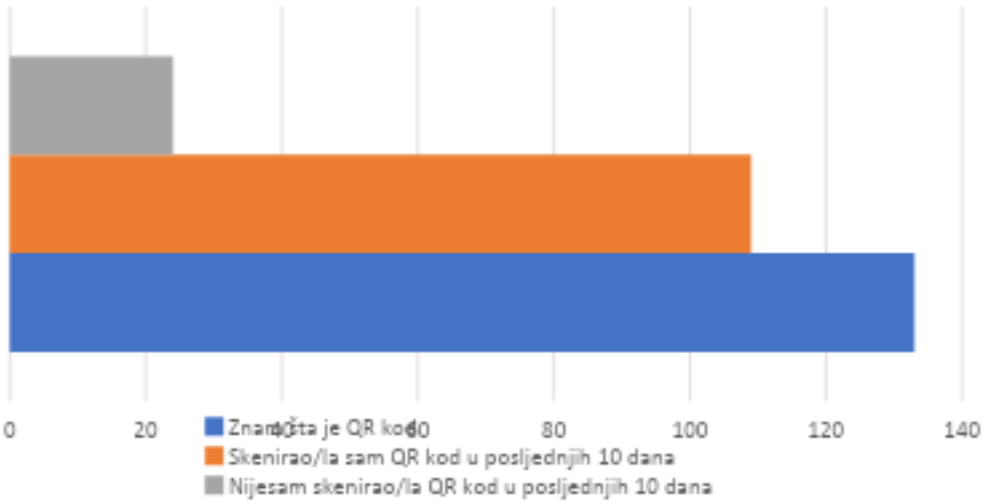
Grafik 6. Zastupljenost IT stručnjaka među učesnicima ankete

Da li ste imali priliku da skenirate neki QR kod u posljednjih 10 dana?

Na ovo pitanje je dalo odgovor 139 osoba od kojih je 109 odgovorilo potvrdno, dok je „NE“ odgovorilo 30 osoba. Ova informacija ukazuje na učestalu potrebu korišćenja QR kodova.

Grafik 7. Učestalost skeniranja QR kodova u posljednjih 10 dana

Od ukupno 133 ispitanika/ce koji su odgovorili da su upoznati sa pojmom QR kodova njih 109 je odgovorilo da je u posljednjih 10 dana skeniralo neki QR kod.



Grafik 8. Procentualni prikaz odgovora na pitanje "Da li ste imali priliku da skenirate neki QR kod u posljednjih 10 dana?"

3.4 Opšta informisanost o informacionoj bezbjednosti

U ovoj sekciji osobe koje su učestvovale u anketi davale su odgovore na pitanja o opštoj informisanotsti o informacionoj bezbjednosti, kao i o svjesnosti da postoje određene prijetnje u sajber prostoru kroz prizmu fišing napada.

1. Da li ste upoznati sa činjenicom da postoji opasnost na Internetu?
2. Da li ste upoznati sa pojmom fišing napada?
3. Ukoliko je na prethodno pitanje Vaš odgovor „Da“, da li možete objasniti šta je ili navesti neki primjer fišing napada?
4. Da li ste imali priliku da budete „žrtva“ fišing napada?
5. Ukoliko je na prethodno pitanje Vaš odgovor bio „Da“, da li možete da napišete na koji način je izvršen napad, putem elektronske pošte, društvenih mreža, SMS poruke ili nešto drugo?
6. Da li smatrate da ste dovoljno informisani o rizicima koji postoje u sajber prostoru?
7. Da li ste nekada u privatnom ili poslovnom životu imali priliku da prisustvujete nekom treningu ili obuci o važnosti sigurnosti na Internetu?

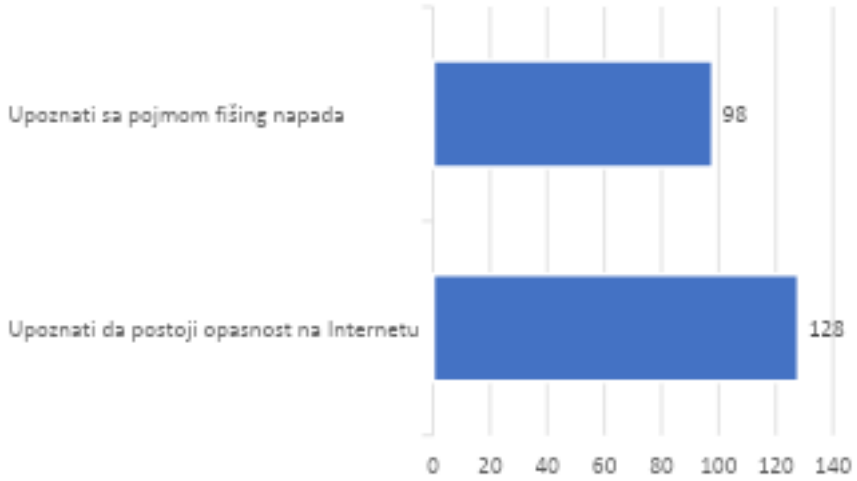
Da li ste upoznati sa činjenicom da postoji opasnost na Internetu?

Prvo pitanje u sekciji koja se odnosi na sajber bezbjednost, svi učesnici ankete su dali odgovor i 13 učesnika/ca je odogovorilo da nije svjesno da postoji određena opasnost na Internetu.

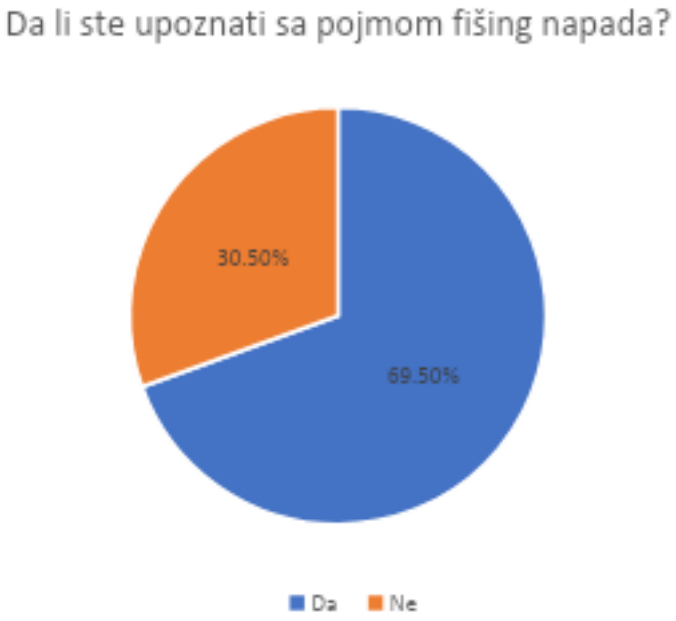
Grafik 9. Upoznatost učesnika/ca sa rizicima na Internetu

Da li ste upoznati sa pojmom fišing napad?

Svi učesnici/e ankete su dali odgovor na pitanje o pojmu fišing napada, a njih 98 je odgovorilo sa „Da“, dok je 43 učesnika/ce ankete odgovorilo sa „Ne“. Napravljena je paralela u odgovorima o upoznatosti sa samim pojmom informacione bezbjednosti i fišing napada i razlika je u 30 odgovora.



Grafik 10. Poređenje svijesti o opasnostima na Internetu i poznavanja fišing napada među učesnicima



Grafik 11. Grafički prikaz odgovora na pitanje "Da li ste upoznati sa pojmom fišing napad?''

Da li možete objasniti ili dati primjer fišing napada?

Četrdeset učesnika/ca ankete je dalo odgovor na ovo pitanje u vidu tekstualnog obrazloženja a primjeri koji se najčešće prožimaju kroz odgovore jesu:

- Email,
- SMS,
- Pozivi,
- URL adrese poslate preko društvenih mreža.

Određeni broj učesnika/ca ankete dao je i primjere poput:

- Clickbait,
- QR kod,
- Online shoping.

Nekoliko učesnika/ca prilično tačno je definisalo fišing napade ili objasnilo na primjeru:

- „Lažno predstavljanje u cilju lakšeg pridobijanja informacija kao sto su lozinke, platne kartice,…“
- „ Fišing napad-Internet prevara tj. pokušaj prikupljanja ličnih podataka.
- Najčešće se vrši putem slanja SMS ili E-mail poruka kako bi se ostvarilo prikupljanje novca za tudjih bamkovnih racuna.“
- „Određeni broj fišing napada ima za cilj krađu kredencijala, dok ostali imaju za cilj distribuciju zlonamjernog softvera. Neki od primjera zahtijevanih radnji u fišing napadima su sljedeći: Klik na određeni link, Ažuriranje lozinke..“
- „Clickbait napad đe se nudi određeni proizvod, roba ili usluga putem reklamno-propagandnog materijala (reklame, video snimka sa linkom, fb/ig stranice) kako bi se prikupili/zloupotrijebili lični podaci korisnika/"kupca" (Jedinstveni matični broj građanina, Broj kreditne kartice, broj ličnog dokumenta, fotografija lica), a koji bi se kasnije upotrijebili za razne svrhe (možda čak i nezakonite) mimo znanja tog lica od kojih su uzeti/ukradeni podaci.“
- „Mailovi u kojima se pošiljaoc predstavlja kao firma u kojoj ste vi nekad nešto kupili, račun treba da se provjeri što se može uraditi klikom na link koji vam pošalju. Što dalje vodi do krađe vaših podataka“.

Da li ste nekada bili žrtva fišing napada?

Na pitanje o iskustvu sa fišing napadima odogovorilo je 95% ispitanika/ca a njih 9.5% je odgovorilo da jeste dok je 124 odnosno 90.5% odgovorilo da nije iskusilo napad fišera.

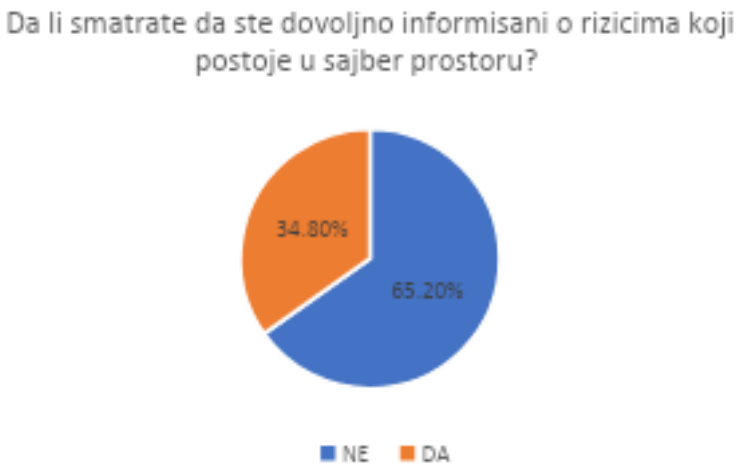
Od 9.5% ispitanika/ca koji su odgovorili da su bili žrtve fišing napada najviše ih je odgovorilo da su napad doživjeli putem SMS poruke i e-mail-a.

- „Putem aplikacija za komunikaciju u nekoliko navrata sam dobijao poruku da pošiljka koju sam navodno poručio ne može da stigne dok ne unesem podatke na lažiranoj stranici Pošte Crne Gore. Stranica nije imala https. Drugi pokazatelj je bio jezik i stil teksta koji je bio pun grešaka, djelo Google translatora, vjerovatno.“

Grafik 12. Procenat učesnika koji su prijavili iskustvo sa fišing napadom

Da li smatrate da ste dovoljno informisani o rizicima koji postoje u sajber prostoru?

Na pitanje o tome da li smatraju da su dovoljno informisani o rizicima koji postoje u sajber prostoru svi učesnici/ce ankete su dali odgovor a većina njih je dala negativan odgovor na pitanje.



Grafik 13. Stepen informisanosti učesnika/ca o rizicima u sajber prostoru.

Da li ste nekada u privatnom ili poslovnom životu imali priliku da prisustvujete nekom treningu ili obuci o važnosti sigurnosti na Internetu?

Na pitanje da li su nekada prisustvovali nekom treningu ili obuci na kojoj bi se upoznali o važnosti sigurnosti na Internetu, ponovo je većina učesnika/ca ankete odgovorilo negativno. Čak 54.7% od ukupnog broja izjavilo je da nikada ni u privatnom ni u poslovnom životu nije imalo priliku da se susretne sa sličnom obukom.

Grafik 14. Udio učesnika/ca sa iskustvom u obukama o važnosti sigurnosti na Internetu, u privatnom ili poslovnom kontekstu

3.5 QR kodovi kao fišing sredstvo

Posljednji set pitanja, nakon što su ispitanici/e odgovorili na pitanja opšte informisanosti o QR kodovima i fišing napadima spaja ove dvije kategorije i ima cilj provjeru da li su korisnici Interneta upoznati da se sve više fišing napada dešava upravo posredstvom skeniranja QR kodova, ali i da podigne nivo svijesti o ovoj temi na taj način.

Pitanja su koncipirana sljedećim redosljedom:

1. Da li ste upoznati sa činjenicom da postoje bezbjednosni rizici skeniranjem QR kodova?
2. Da li ste imali priliku da se susretnete sa QR kodom nakon čijeg skeniranja ste pozvani na neku akciju poput registracione forme, preuzimanja nekog fajla, aplikacije ili slično.
3. Da li ste nekada, nakon što ste skenirali QR kod, ostavili svoje lične podatke na nekoj registracionoj formi, bez da ste provjerili šta će se dalje desiti sa njima, da li će biti zloupotrijebljeni?
4. Da li ste nekada, nakon što ste skenirali neki QR kod, preuzeli neku aplikaciju sa neprovjerene lokacije (a da to nije Play store/App store)?
5. Da li ste nekada preduzeli neku dodatnu mjeru zaštite prije nego što ste skenirali QR kod?
6. Ukoliko je Vaš odgovor na predhodno pitanje bio „Da“, da li nam možete reći o kojoj provjeri je riječ?

Odgovarajući na ova pitanja, ispitanici su dali jasnu sliku o tome koliko su korisnici na Internetu svjesni opasnosti koja se krije iza naizgled bezopasnih QR kodova i koliko je sigurnost zapravo ugrožena.

Da li ste upoznati sa činjenicom da postoje bezbjednosni rizici skeniranjem QR kodova?

Prvim postavljenim pitanjem u ovom dijelu ankete provjerava se uopštena svjesnost korisnika o bezbjednosnim rizicima koji postoje skeniranjem QR kodova. Ispitanici/e su dali polovičan odgovor na ovo pitanje, više od polovine ukupnog udjela učesnika u anketi je odgovorilo da nije svjesno ove opasnosti, dok je 46.80% dalo potvrdan odgovor na ovo pitanje.

Grafik 15. Svjesnost ispitanika/ca da o rizičnosti skeniranja QR kodova

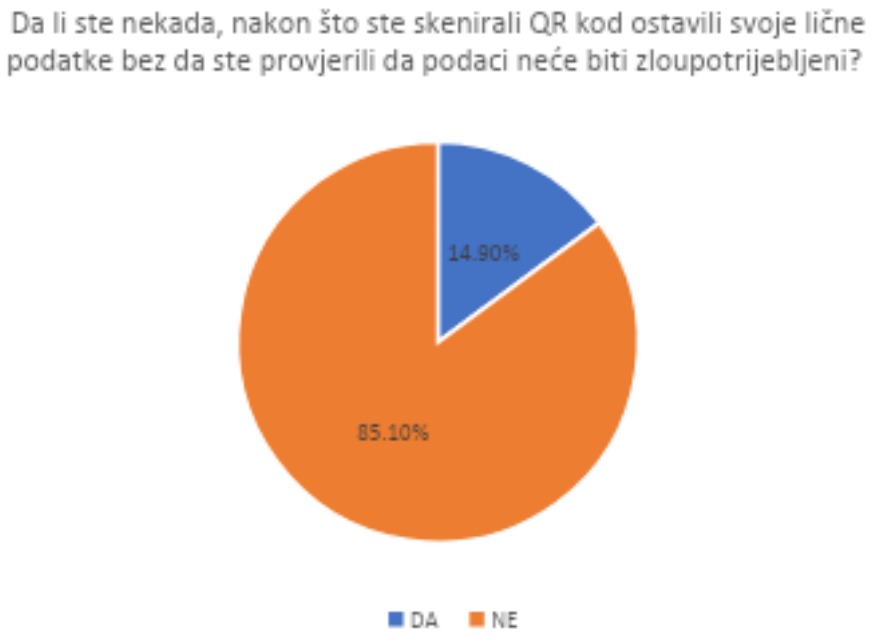
Da li ste imali priliku da se susretnete sa QR kodom nakon čijeg skeniranja ste pozvani na neku akciju; npr. registraciona forma, preuzimanje fajla ili neke aplikacije ili slično?

Na pitanje da li su se nekad sreli sa QR kodom koji "poziva na akciju", odnosno sa QR kodom koji nije samo statični prikaz, recimo jelovnika iz restorana većina ispitanika dala je negativan odgovor. Ipak, nije zanemarljiv broj učesnika ankete koji su dali suprotan odgovor, njih 50.

Grafik 16. Udio učesnika koji su se susreli sa QR kodovima koji pozivaju na akciju

Da li ste nekada, nakon što ste skenirali neki QR kod, ostavili svoje lične podatke bez da ste provjerili da podaci neće biti zloupotrijebljeni?

Na pitanje 'Da li ste nekada, nakon što ste skenirali neki QR kod, ostavili svoje lične podatke bez da ste provjerili da podaci neće biti zloupotrijebljeni?', gotovo 15% ispitanika odgovorilo je potvrdno. Ovaj procenat ukazuje na zabrinjavajući nivo povjerenja u QR kodove i nedostatak opreza među korisnicima, što ih može učiniti podložnijima zloupotrebama i potencijalnim fišing napadima.



Grafik 17. Procenat učesnika koji su ostavili lične podatke bez provjere njihove sigurnosti nakon skeniranja QR koda

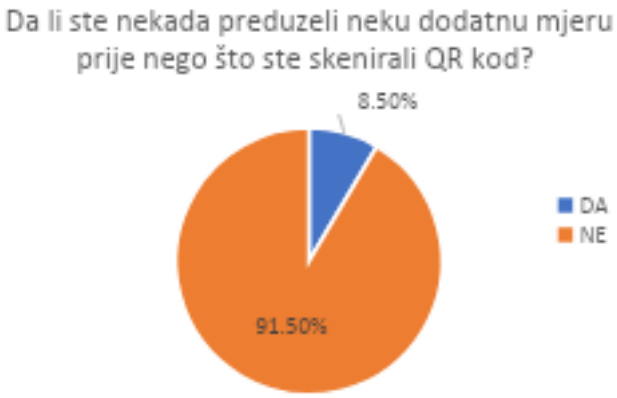
Da li ste nekada, nakon skeniranja QR koda preuzeli neku aplikaciju sa neprovjerene lokacije (osim Play prodavnice/App prodavnice)

Određeni broj aplikacija popularnih u svijetu još uvijek je nedostupan u Crnoj Gori. Uzmimo za primjer globalno popularnu društvenu mrežu *Snapchat* koja je tek prije pola dekade postala dostupna korisnicima u Crnoj Gori putem Play prodavnice i App prodavnice, a godinama prije toga su je tinejdžeri preuzimali sa piratskih sajtova za preuzimanje. Usput su, jako često "zakačili" i neki virus. Upravo iz razloga što neke aplikacije nijesu dostupne u našoj zemlji, korisnici na Internetu su podložni preuzimanju sa piratskih sajtova putem web pregledača koji često nemaju adekvatne sigurnosnosne standarde. Iz tog razloga ne čudi činjenica da je čak 20% ispitanika/ca dalo potvrdan odgovor na ovo pitanje.

Grafik 18. Odgovori učesnika/ca ankete o preuzimanju aplikacija sa piratskih sajtova

Da li ste nekada preduzeli neku dodatnu mjeru prije nego što ste skenirali QR kod?

Da su bezbjednosni standardi na jako niskom nivou i da je potrebno podizanje svijesti korisnika Interneta kakva opasnost se krije iza QR kodova, najbolje potvrđuje činjenica da je samo 12 od 141 ispitanika/ce odgovorilo da je preduzelo dodatnu mjeru prije skeniranja QR koda.



Grafik 19. Procenat učesnika koji su preduzeli mjere opreza prije skeniranja QR koda

Ukoliko je vaš odgovor na prethodno pitanje bio "DA", da li nam možete reći o kojoj provjeri je riječ?

Posljednje pitanje na anketi odnosi se na sigurnosnosnu provjeru prije skeniranja QR koda. Malobrojni učesnici ankete, koji su odgovorili da provjere prije nego što skeniraju QR, kod dali su sljedeće odgovore:

- Web stranica,
- Internet provjera,
- Provjerio vjerodostojnost te aplikacije na zvaničnim nalozima prodavnica,
- Provjerila odakle je QR kod,
- Provjerila da li je to zvanični sajt,
- Provjera provajdera QR koda, zvanične Web stranice i sl.

Dodatno, anketirani učesnici su dali sugestije za dalji rad:

- „Fali nam više predavanja i obuka vezanih za sajber kriminal i Internet prevare.“
- „Mislim da je ova tema važna i da je nepoznanica ovog društva“
- „Trebamo više raditi i učiti o QR kodu, jer se susrećemo u svakodnevnici sa njim.“

3.6 Kvalitativna analiza ankete u odnosu na posebne kategorije

Da bi izveli kvalitativnu analizu rezultata ankete u vezi sa postavljenim pitanjima, podatke prikupljene anketom ćemo podijeliti u odnosu na sociološke podkategorije. Na osnovu sociooloških kategorija, analizirani su odgovori prema:

- Starosnoj dobi ispitanika/ca,
- Polu,
- Nivou obrazovanja,
- Oblasti zanimanja,
- IT stručnjacima kao podkategoriji zanimanja.

Za kvalitativnu analizu rezulata ankete iskorišćena su sljedeća pitanja:

- Da li ste upoznati sa pojmom fišing napad?

  Istraženo je kako različite demografske grupe odgovaraju na pitanje vezano za poznavanje samog pojma fišing napada.
- Da li smatrate da ste dovoljno informisani o rizicima koji postoje u sajber prostoru?

  Napravljena je analiza svijesti o rizicima u sajber prostoru među različitim grupama.

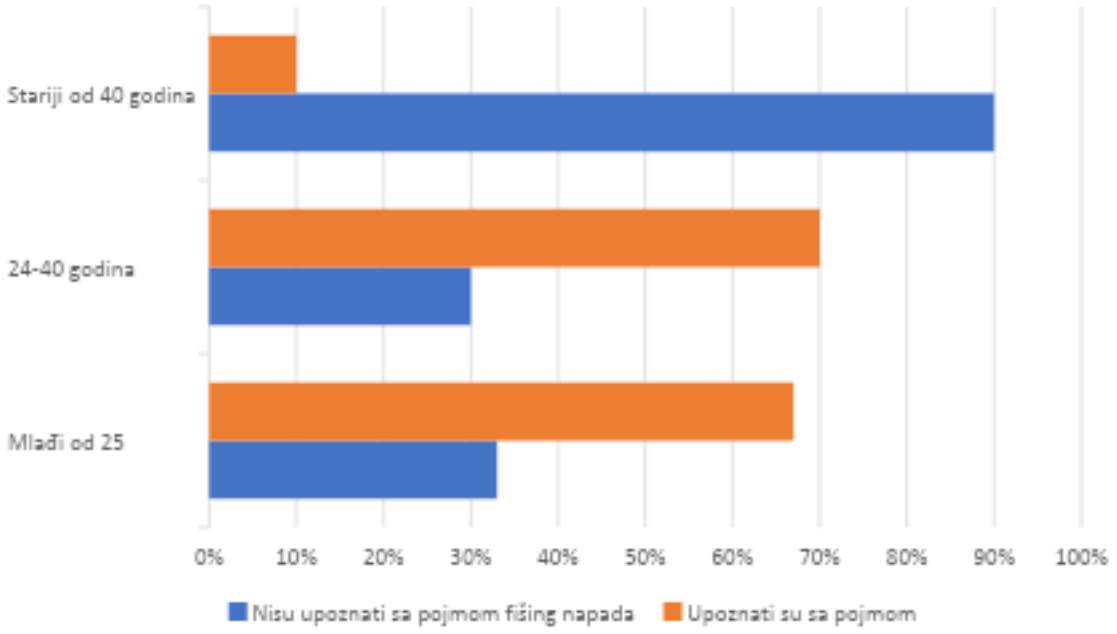
- Da li ste nekada imali priliku da prisustvujete nekom treningu ili obuci o sajber bezbjednosti?
  Ova analiza biće od izuzetne važnosti za buduća istraživanja na temu.
- Da li ste znali da postoje bezbjednosni rizici skeniranja QR koda?
  Napravljena je analiza ranjivosti grupa na osnovu svjesnosti rizika skeniranja QR koda.
- Da li ste ikada, nakon što ste skenirali QR kod preuzeli neku aplikaciju sa neprovjerene lokacije (a da to nije Play store/App store)?
- Da li ste nekada preduzeli neku dodatnu mjeru prije nego što ste skenirali QR kod?

Rezultati ankete u odnosu na posebne kategorije

Anketa je pokazala da su određene grupe "ranjivije" kada je u pitanju sigursnost skeniranja QR kodova, ali i generalno sigurnost na Internetu.

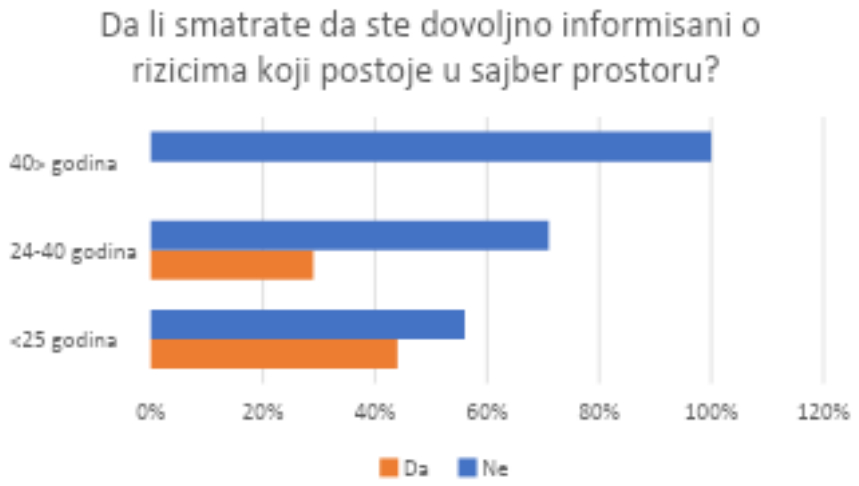
Analiza prema starosnm grupama

Na pitanje: „Da li ste upoznati sa pojmom fišing napad?“ odgovor „Ne“ odabran je, u odnosu na starosne grupe na sljedeći način:



Grafik 20. Raspodjela odgovora na pitanje o upoznatosti sa fišing napadima prema starosnim grupama

Na grafiku 20. prikazani su procenti kako su ispitane osobe u anketi odgovorile na pitanje „Da li ste upoznati sa pojmom fišing napada?“, iz prikazanog vidi se da oko 70% pripadnika mlađe populacije je odgovorilo sa „Da“ na ovo pitanje, dok su gotovi svi (90%) ispitanika/ca starije populacije odgovorili sa „Ne“.



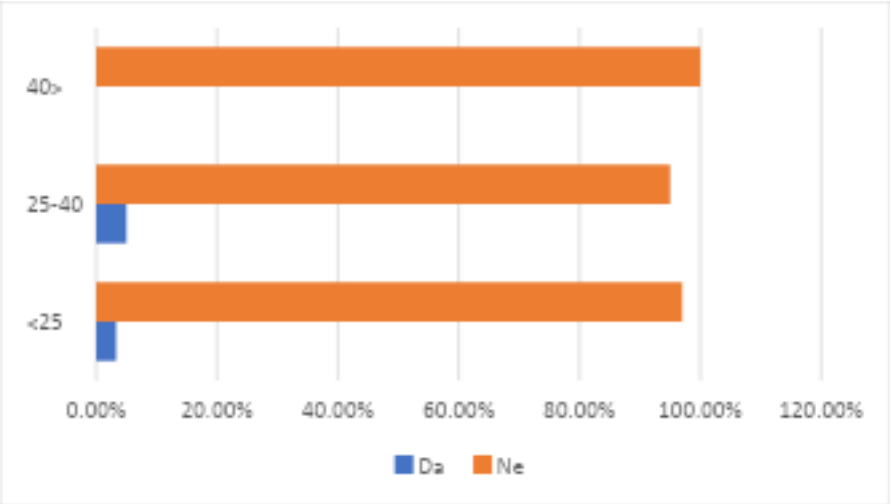
Grafik 21. Raspodjela odgovora o informisanosti o rizicima u sajber prostoru prema starosnim grupama

Većina starije populacije odgovorilo je da se do sada nije susrelo sa obukom ili treningom iz sajber bezbjednosti. Preko 50% učesnika/ca ankete starosne dobi 24-40 godina dalo je negativan odgovor, dok je duplo manje učesnika mlađih od 25 godina koji se nisu susreli sa navedenom obukom ili treningom.

Grafik 22. Rezultati po starosnim grupama na pitanje o obukama i treninzima iz sajber bezbjednosti

Grafik 23. Rezultati prema starosnoj dobi na pitaje o svjesnosti da skeniranje QR kodova nosi određene rizike

Sličan zaključak kao kad je u pitanju obuka o bezbjednosti na Internetu može se donijeti i na osnovu poređenja odgovora o svjesnosti rizičnosti skeniranja QR kodova prema grupama. Niko od učesnika/ca ankete starijih od 40 godina nije odgovorio sa "Da". Većinom "Ne" je odgovorila većina koja pripada starosnoj dobi između 25 i 40 godina dok je najmlađa populacija većinom upoznata sa rizikom. Ovaj rezultat najbolje pokazuje efikasnost govora i promovisanja informacione bezbjednosti među korisnicima.



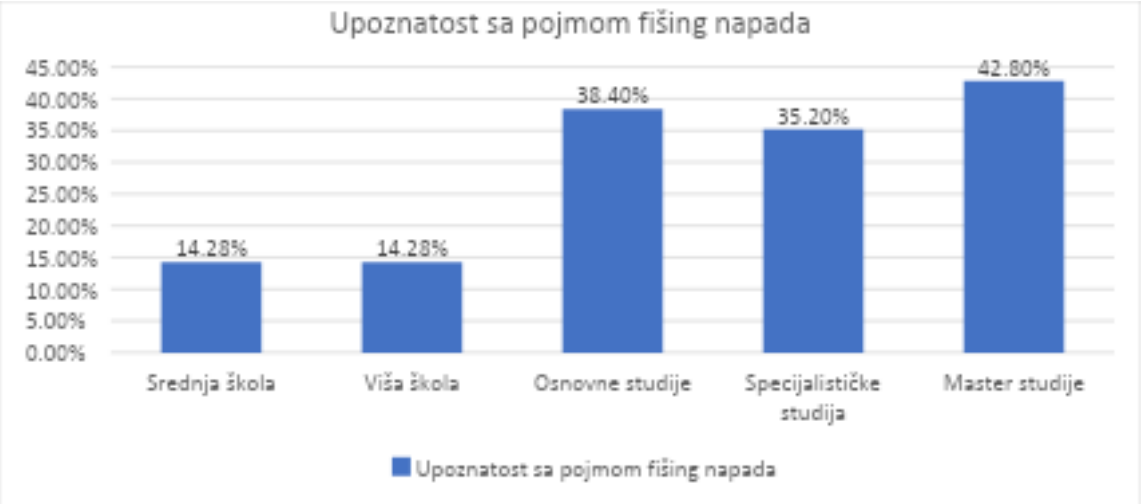
Grafik 24. Da li ste nekada preduzeli neku dodatnu mjeru prije nego što ste skenirali QR kod?

Na kraju, iako je najmlađa grupa većinom odgovorila da je svjesna da postoji određeni rizik kod skeniranja QR kodova, manje od 5% učesnika ankete dalo je potvrdan odgovor na pitanje da li su preduzeli neku dodatnu sigurnosnu mjeru prilikom skeniranja QR koda. Sličan odgovor je i kod srednje starosne grupe a rezultati ankete pokazali su da je najranjivija grupa starijih od 40 godina.

Analiza prema stepenu obrazovanja

Na pitanje „Da li ste upoznati sa pojmom fišing napada?“, niko od učesnika/ca ankete sa posljednje završenim nivoom obrazovanja osnovna ili srednja škola nije dao potvrdan odgovor.

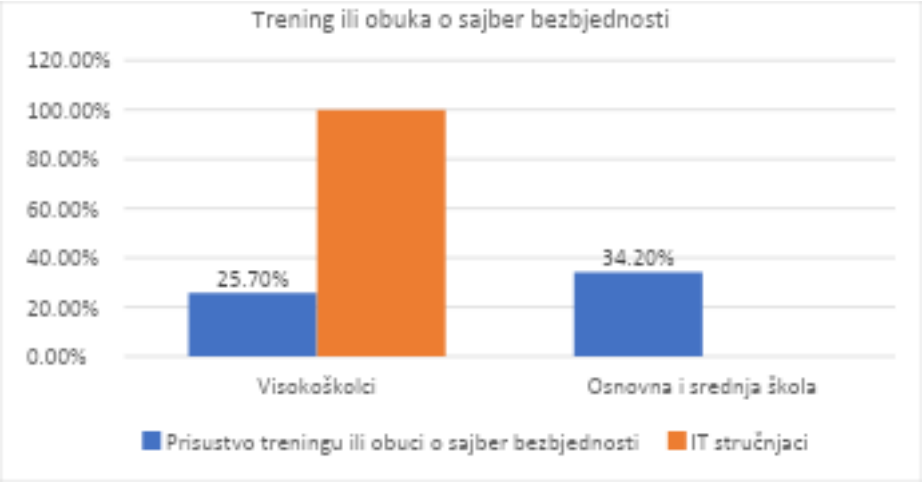
38.40% od ukupnog broja učesnika koji su završili osnovne studije odgovorilo je da je upoznato sa pojmom fišing napad. Na pitanje o upoznatosti sa pojmom fišing napada 42.8% svršenika master studija je dalo potvrdan odgovor, 58.2% se izjasnilo da nije upoznato sa ovim pojmom. Kada je riječ o osobama čiji je posljednji završeni obrazovni nivo specijalističke studije njih 35.2% dalo je potvrdan odgovor dok je negativno odgovorilo 64.8%. Nijedan učesnik ili učesnica ankete koji su odgovorili da su posljednje završili osnovnu školu nije odgovorio/la da je upoznat/a sa ovim pojmom dok je 14.28% od ukupnog broja osoba sa posljednje završenom srednjom i višom školom dalo odgovor da je upoznato sa fišing napadom. Kada je riječ o visokoškolcima koji su se izjasnili da dolaze iz IT oblasti 80% njih je dalo potvrdan odgovor na pitanje.



Grafik 25.Upoznatost sa pojmom fišing napad prema obrazovnoj strukturi

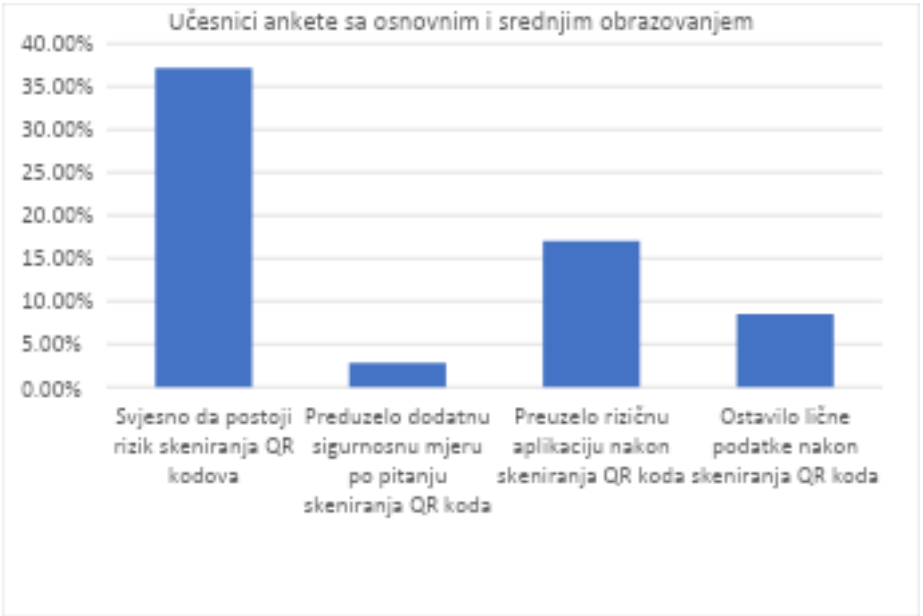
Odgovori na ovo pitanje su jasan indikator da je potrebno više zastupljenosti priči o sajber bezbjednosti u osnovnim i srednjim školama, ali ako uzmemo u obzir da je 77% visokoškolaca dalo negativan odgovor na ovo pitanje jasno je da je potrebno više riječi o sajber bezbjednosti i na fakultetima.

Na pitanje "Da li ste nekada u privatnom ili poslovnom životu imali priliku da prisustvujete nekom treningu ili obuci o sajber bezbjednosti?", 25.7% visokoškolaca (viša škola, osnovne studije, specijalističke ili master studije) dalo je potvrdan odgovor. Svi IT stručnjaci su dali potvrdan odgvor dok je 32% visokoškolaca koji ne dolaze iz IT-a odgovorilo da se do sada nije susrelo sa treningom ili obukom o sajber bezbjednosti. 34.2% osoba sa završenom osnovnom ili srednjom školom odgovorilo je da je imalo priliku da pristustvuje nekoj obuci ili treningu o sajber bezbjednosti.



Grafik 26. Prisustvo treningu ili obuci iz sajber bezbjednosti prema obrazovnoj strukturi

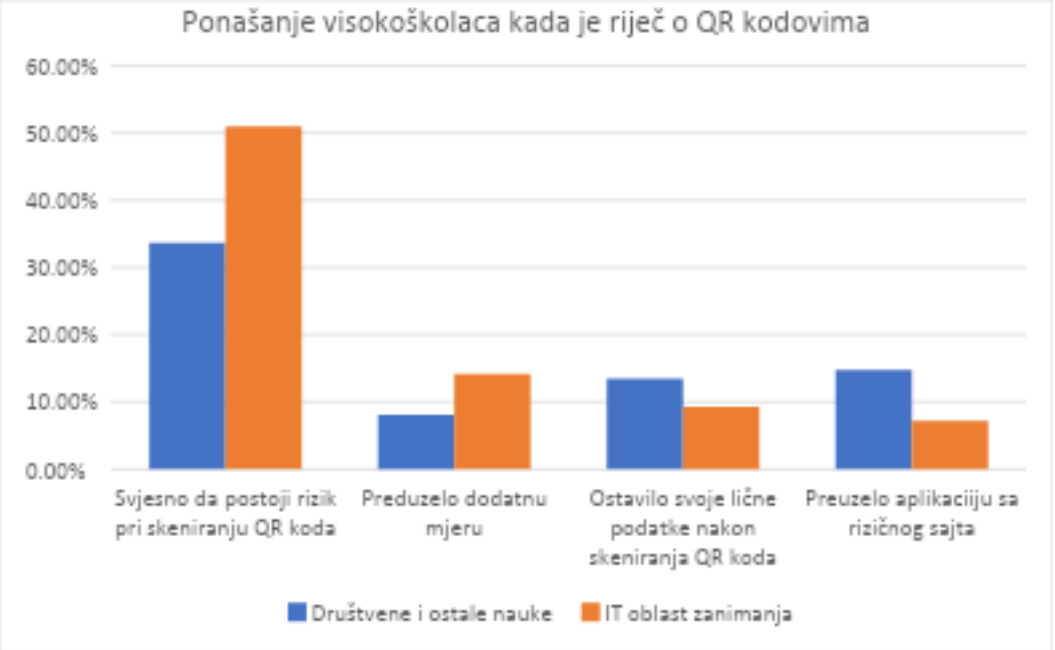
37.14% osoba sa posljednje završenom osnovnom ili srednjom školom odgovorilo da je da je svjesno da postoji rizik pri skeniranju QR kodova, ali samo 2.8% među njima je odgovorilo da preduzima neke dodatne mjere prije skeniranja QR koda dok je 17% njih odgovorilo da je nakon skeniranja QR koda preuzelo neku aplikaciju sa prodavnice koja nije Play ili App store, a 8.5% je ostavilo svoje lične podatke nakon što je skeniralo QR kod a da nijesu bili sigurni da isti neće biti zloupotrijebljeni.



Grafik 27. Odgovori o sigurnom ponašanju pri skeniranju QR kodova obrazovne strukture osnovna i srednja škola

Kada je riječ o visokoškolcima čija struka nije informacione tehnologije, njih 33.7% je odgovorilo da je upoznato sa bezbjednosnim rizicima skeniranja QR kodova. Njih 8.1% odgovorilo je da je nekad preduzelo neku dodatnu mjeru pri skeniranju QR koda, a 13.5% je ostavilo svoje lične podatke bez provjere. Na pitanje "Da li ste ikada, nakon što ste skenirali QR kod preuzeli neku aplikaciju sa neprovjerene lokacije (a da to nije Play store/App store)?", potvrdno je odgovorilo njih 14.8%.

51% osoba koje su učestvovale u anketi a dio su IT zajednice upoznato je sa potencijalnim bezbjednosnim rizicima skeniranja QR koda, njih 14.2% je nekada i preduzelo neku sigurnosnu mjeru pri skeniranju QR koda ali je 7.2% preuzelo neku aplikaciju sa prodavnice koja nije zvanična odnosno 9.3% ostavilo svoje podatke bez provjere.



Grafik 28. Uporedni grafik visokoškikaca iz IT i ostalih struka po pitanju ponašanja pri skeniranju QR kodova

Uzevši u obzir da je 100% učesnika ankete IT smjera prisustvovalo nekoj sajber bezbjednosnoj obuci ili treningu a da je nešto više od 8% pokazalo rizično ponašanje kada su QR kodovi u pitanju, jasno je da je edukacija najefektniji vid zaštite građana.

3.7 Uporedna analiza fišing napada u svijetu i u Crnoj Gori

Opasnost od skeniranja QR kodova postoji svuda u svijetu, ne samo u Crnoj Gori. Nacionalni centar za sajber bezbjednost Velike Britanije na svom zvaničnom sajtu (www.ncsc.gov.uk/) objavio je tekst kojim poziva građane na opreznost kada je skeniranje QR kodova u pitanju. U tekstu se navodi da su QR kodovi postali široko popularni za vrijeme pandemije korona virusa i da se danas koriste za naručivanje hrane, provjeru statusa vakcinacije, itd. Oni navode da se QR prevare najčešće dešavaju u otvorenim prostorima poput autobskih stajališta najčešće uključujući socijalni inženjering. Kao razlog za povećani broj fišing napada putem QR kodova navodi se da su ljudi sada oprezniji prema sumnjivim linkovima u emailovima, pa kriminalci koriste QR kodove da sakriju maliciozne linkove. Preporučuje se i korišćenje ugrađenog QR skenera na mobilnom telefonu, a ne aplikacije preuzete iz prodavnica aplikacija [28].

Zvanični sajt informacione bezbjednosti vlade Kanade (www.getcybersafe.gc.ca) takođe ukazuje na opasnost skeniranja QR kodova. Oni savjetuju građane da preuzimaju aplikacije samo sa provjerenih prodavnica, da se suzdržavaju od dijeljenja informacija putem linkova sa QR kodova kao i da ne prave nikakve transakcije putem QR kodova. [27].

Rizici koje skeniranje QR kodova nosi prepoznati su i u Crnoj Gori. Na zvaničnom sajtu Vlade Crne Gore (www.gov.me) nalazi se tekst pod nazivom „Skriveni rizici upotrebe QR kodova“ u kome se navodi da se QR kodovi najčešće koriste u plaćanju i bankarstvu, marketingu i oglašavanju, te kao vodič za muzeje i turističke atrakcije. Na sajtu se navodi da maliciozni QR kodovi mogu biti široko distribuirani putem naljepnica, bilborda ili elektronskih poruka i da mogu preusmjeriti korisnike na zlonamjernu veb stranicu koja može ukrasti lične podatke. Na sajtu se poziva i na opreznost u skeniranju QR kodova kao i dijeljenja ličnih podataka [29]. Tekst je objavljen u septembru 2023. godine, a u Nacrtu strategije sajber bezbjednosti Crne Gore od 2022-2026. nema podataka o rizicima skeniranja QR kodova. Anketnim istraživanjem sprovedenim u okviru rada utvrđeno je da više od 54% učesnika/ca ankete se do sada nije susrelo sa nekim treningom ili radionicom iz sajber bezbjednosti, a u Nacrtu strategije sajber bezbjednosti Crne Gore edukacija se navodi kao strateški i operativni cilj za period od 2022. do 2026. godine [29].

Na sajtu Vlade Crne Gore bankarstvo se navodi kao najčešća oblast korišćenja QR kodova [28], a prema APWG-u upravo je sektor finansija najviše pogođen QR fišing napadima u prvom kvartalu 2022. godine [30]. Logistika, plaćanja, društvene mreže i kripto valute, takođe su prepoznate sa velikim procentom kada je riječ o napadima izvedem putem QR kodova [30].

4. Eksperiment – koliko su korisnici na Internetu zaista obazrivi kada je je skeniranje QR kodova u pitanju

U februaru 2024. godine na konferenciji u San Dijegu u Kaliforniji istraživači Filipo Sharevski, Mattia Mossano i Gunther Schiefer predstavili su rezultate svog eksperimenta fišinga putem QR kodova u okviru kojeg su došli do sljedećih saznanja:

„QR kodovi, dizajnirani za praktičan pristup vezama, nedavno su prisvojeni kao vektori fišing napada. Budući da je ova vrsta krađe identiteta relativna i da su mnogi aspekti prijetnje u stvarnim uslovima nepoznati, proveli smo studiju u prirodnim okruženjima (n=42) kako bismo istražili kako se ljudi ponašaju oko QR kodova koji bi mogli sadržavati veze za krađu identiteta.“

- Od ukupno 42 učesnika u eksperimentu, njih 28 ili 67% je otvorilo URL link na koji ih je uputio skenirani QR kod bez ikakve provjere linka koji otvaraju.

Istraživači su koristili koncept humanitarne akcije po kojoj bi učesnici skenirnajem QR koda postali učesnici u samoj akciji.

- 52% učesnika ili njih 22 reklo je da je bilo dovoljno da samo pročitaju naslov i povjeruju da će zaista učestvovati u humanitarnoj akciji skeniranjem QR koda.
- Samo 8% učesnika eksperimenta je napustilo URL adresu nakon što je posumnjalo u vjerodostojnost iste.
- 44% učesnika je napustilo URL adresu nakon što su vidjeli da se u istoj nalazi riječ "phishing". [24]

Druga naučna studija

Rezultati slične studije prikazani su i na De Paul univerzitetu u aprilu 2022. godine. Grupa od četvoro istrživača prikazala je rezultate svog eksperimenta koji su nazvali "Quishing".

Ideja započinje upravo u trenutku kada su QR kodovi kao sredstvo beskontaktnog pristupa informacijama dobili i svoju najveću popularnost – za vrijeme pandemije virusa Covid-19.

Za vrijeme pandemije mnoge države su za ulazak i pristup većini institucija kao i za boravak na zatvorenim javnim površinama uvele obaveznu potvrdu o vakcinaciji. Grupa koja je sprovela istraživanje je učesnicima u eksperimentu prikazala da će skeniranjem QR koda biti preusmjereni na aplikaciju u koju se potrebno prijaviti kako bi potvrda o vakcinaciji bila validna. Učesnici u eksperimentu su se na toj lažnoj aplikaciji prijavljivali putem svog Facebook naloga, putem svog Google naloga ili su samostalno kreirali svoje naloge.

Korisnički interfejs aplikacije prikazan je na slici ispod.

Slika 25. Korisnički interfejs aplikacije korišćene u istraživanju

- Od 173 učesnika u eksperimentu, njih 44.5% je izabralo da se na aplikaciju prijavi pomoću svog Google naloga
- Njih 22.5% je odabralo da se prijavi koristeći Facebook nalog (iako je ponuđen kao prva opcija)
- 18.5% je odabralo da napravi novi korisnički nalog
- Samo 14.5% je odabralo da preskoči korak kreiranja naloga i ostavljanja informacija na ovu aplikaciju.

Kada su u pitanju razlozi zbog kojih su odabrali jedan od načina prijave učesnici su dali sljedeće odgovore:

- „kreiranje potpuno novog naloga je izgledalo kao proces koji će predugo da traje pa sam odabrao da se prijavim putem Facebook-a", kazao je korisnik koji je odabrao Facebook za prijavu
- Neki od učesnika su vodili računa i o sigurnosti: "Preferiram da koristim Facebook kada eksperimentišem sa novim aplikacijama jer ne želim da moj Email bude "zatrpan" neželjenom poštom".
- Samo jedan učesnik je bio sumnjičav da se radi o fišingu preko QR kodova: „Nisam bio siguran da li mogu da vjerujem linku koji je postavljen na QR kodu pa sam se prijavio

putem Facebook naloga i odmah nakon toga promijenio pasvord na svom nalogu na ovoj društvenoj mreži.“

Niko od učesnika istraživanja koji su se prijavili putem Google naloga nije bio sumnjičav a neki od odgovora zašto su iskoristili svoj Google nalog bili su:

- „Ne želim da ovaj vakcinacioni pasoš bude povezan sa mojim Facebook nalogom pa sam odabrao Google.“,
- „Više vjerujem Google-u nego Facebook-u da će čuvati moje podatke.“
- „Aplikacija mi je izgledala sasvim vjerodostojno pa sam odabrao da se prijavim koristeći kredencijale mojeg Google naloga.“

Ostali su rekli da su jednostavno odabrali Google zato što je ovaj način bio najjednostavniji.

Od skromnih 14.5% koji nisu povjerovali aplikaciji i nijesu napravili naloge stigli su odgovori:

- „Ne znam da li je ova stranica vjerodostojna i ne bih da koristim svoju Email adresu da se ne bi ispostavilo da je prevara.“
- „Ne vjerujem ovoj stranici i ne želim da ostavljam svoje lične podatke, iako izgleda kao zvaničan vladin sajt, kad bolje pogledate, ipak nije!“. [24]

4.1 Eksperiment – sigurnost skeniranja QR kodova u Crnoj Gori

U okviru istraživanja sproveden je eksperiment koji za cilj ima uporednu analizu odgovora koje su dali učesnici ankete i realnog stanja. Eksperimentalni scenario bio je zamišljen tako da obuhvati više različitih lokacija kako bi se istražilo ponašanje korisnika u realnim životnim situacijama. QR kodovi su postavljeni na različitim javnim mjestima u Podgorici i Plavu uključujući kafiće, stajališta gradskog prevoza, prodavnice i parkove. Na svakom od ovih mjesta QR kod je bio dio plakata koji je simulirao humanitarnu akciju čime je privukao pažnju korisnika (u ovom slučaju slučajnih učesnika eksperimenta). Cilj eksperimenta bio je da se prate reakcije korisnika na skeniranje QR kodova, kako bi se izmjerila njihova obazrivost i spremnost da skeniraju QR kod bez prethodne provjere. Eksperiment je vršen u periodu od 01.03.2024. godine do 01.05.2024.

Slika 26. Izgled plakata korišćenog u okviru eksperimenta

Na formi je bio tekst *"Hvala na učestvovanju u eksperimentu koji se sprovodi u okviru master rada "* ***ANALIZA BEZBJEDNOSNIH RIZIKA PRI UPOTREBI QR KODOVA – STUDIJA SLUČAJA: FIŠING NAPADI" na Univerzitetu Crne Gore. Ovim skeniranjem pomažete u istraživanju. Ukoliko želite da učestvujete u humanitarnoj akciji posjetite sajt budihuman.me.***

Budite oprezni sa skeniranjem neprovjerenih QR kodova.

Ukoliko želite još uvijek da pomognete ovom istraživanju Vaš odgovor na pitanje "Šta vas je privuklo da skenirate ovaj QR kod bi bio jako značajan! Hvala!"

QR kod je skeniran 86 puta u ovom periodu a 23 je dalo odgovor na pitanje.

Najreprezentativniji odgovori su dati ispod:

- Navikao sam da koristim QR kodove bez pretjeranog razmišljanja, a ovaj za humanitarnu akciju mi je izgledao kao sjajna prilika da nekome i pomognem.
- Uvijek skeniram QR kodove koji obećavaju da će me informisati o korisnim stvarima, kao što je humanitarna akcija.

- QR kodovi su savremena tehnologija koju rado koristim, a humanitarna akcija je djelovala kao razlog više za skeniranje.
- Natpis "HUMANITARNA AKCIJA" me je privukao, pa sam skenirala QR kod da vidim o čemu se tu radi.
- Skeniranje QR kodova mi je dio svakodnevnice, pa sam navikao da ih koristim bez previše razmišljanja.
- Skeniram QR kodove svakodnevno, nisam mislila da bi moglo biti išta loše u tome.
- Zanima me šta ova humanitarna akcija konkretno radi.
- Privukla me je ideja da mogu da pomognem skeniranjem koda.
- Trudim se da se odazovem humanitarnim pozivima.
- Ne smatram da QR kodovi mogu da budu opasni.

4.2 Uporedna analiza eksperimenta i ankete

Uporednom analizom odgovora na pitanja iz ankete iz trećeg dijela koje se tiče sigurnosti skeniranja QR kodova i odgovora na eksperimentu sa istim uočavaju se određena odstupanja.

Prema podacima iz ankete:

1. Većina ispitanika zna šta su QR kodovi i koristi ih redovno.
2. Manjina ispitanika preduzima dodatne mjere pre skeniranja QR kodova, a većina to ne čini.
3. Ispitanici sa višim nivoom obrazovanja i oni iz tehničkih nauka češće preduzimaju dodatne mjere kada skeniraju QR kodove.

Rezultati eksperimenta

84 osobe su skenirale potpuno nepoznat QR kod za koji gotovo da nijesu postojale dodatne informacije. Odgovori koje su ostavili pokazuju sljedeće:

1. Naviknuli su da koriste QR kodove i ne razmišljaju previše o tome.
2. Kada je riječ o humanitarnoj akciji ne očekuju da mogu da upadnu u probleme.
3. Vjeruju da QR kodovi ne mogu biti ‘’opasni’’.
4. Svakodnevno skeniraju QR kodove i smatraju ih korisnim.

Upoređivanje dvije grupe:

1. Obije grupe koriste QR kodove i ne razmišljaju o njihovim potencijalnim opasnostima.
2. Učesnici ankete su većinom odgovorili da ne preduzimaju dodatne mjere pri skeniranju QR kodova što je eksperimentalno dokazano.

Na osnovu ankete i eksperimenta ističu se dva glavna pitanja:

1. Da li su korisnici prepoznali potencijalne rizike skeniranja?
2. Koliko korisnika koristi QR kodove redovno.

Većina korisnika se na anketi izjasnila da nije dovoljno informisana o rizicima koje QR kodovi nose. Ovaj podatak dodatno pojašnjava rezultate eksperimenta jer jasno pokazuje da je nesvjesnost o fišing napadima direktno povezana sa neopreznim skeniranjem QR kodova. U vezi s tim, najbolje dobijamo podatke i iz odgovora na pitanje da li i koliko korisnika redovno skenira QR kodove. Većina ispitanika ankete je izjavila da nije upoznata sa fišing napadima (više od 90% starijih ispitanika uopšte nije svjesno rizika) i upravo se ovaj podatak ogleda u eksperimentu gdje je veliki procenat skenirao QR kod bez ikakve prethodne provjere. Iz gore navedenog zaključujemo sljedeće: da korisnici nijesu informisani o rizicima sajber napada i da su kao takvi mnogo podložniji prevarama što je eksperiment jasno i pokazao.

Na osnovu rezultata ankete i eksperimenta možemo i grafički pokazati rezutate:

Tabela 7. Kategorije na osnovu svjesnosti rizika

Kategorija	Broj korisnika	Procenat (%)
Upoznati sa rizicima	28	20%
Nisu upoznati sa rizicima	112	80%
Koristili QR kodove redovno	84	60%

Visoka učestalost korišćenja QR kodova među svim grupama pokazuje popularnost ove tehnologije. Međutim, niska svijest o bezbednosnim rizicima pri skeniranju QR kodova može biti zabrinjavajuća, posebno kod grupe koja skenira QR kodove bez razmišljanja o potencijalnim opasnostima.

Rezultati ankete, kao i rezultati eksperimenta imaju nekoliko sličnosti:

1. Povjerenje u humanitarne akcije

U više odgovora se navodi da humanitarna akcija kao plemeniti čin ne bi trebala biti nešto zabrinjavajuće. Neki korisnici su skenirali QR kod jer im je to izgledalo kao najlakši i najbrži način da nekome pomognu.

- "Navikao sam da koristim QR kodove….kao priliku da nekome i pomognem."
- "Trudim se da se odazovem humanitarnim pozivima."

2. Rutinirana upotreba QR kodova

Mnogo učesnika i ankete i eksperimenta je objasnilo da skeniranje QR koda doživljava kao naviku i da pri tom, ne razmišlja o mogućim rizicima.

- "Skeniram QR kodove svakodnevno, nisam mislila da bi moglo biti išta loše."
- Skeniranje QR kodova mi je svakodnevnica, pa sam navikao da ih koristim bez previše razmišljanja."

3. Tehnološko povjerenje

QR kodove mnogi korisnici prepoznaju kao savremenu tehnologiju u koju imaju povjerenja.

- "Ne smatram da QR kodovi mogu da budu opasni."

Eksperiment je pokazao da je QR kod lako privukao pažnju prolaznika i ovo je najsličnije odgovorima u anketi. Mnogi učesnici nisu previše razmišljali prije skeniranja, što se u potpunosti poklapa sa stavom navedenim u anketi da skeniranje QR kodova postaje rutina.

Na narednom grafiku prikazana je paralela razloga koji su u eksperimentu navedeni kao razlog skeniranja QR koda sa istim razlozima ili odgovorima u okviru ankete.

Grafik 29. Paralelni prikaz sličnih odgovora o QR kodovima u anketi i eksperimentu, x osa predstavlja broj odgovora u anketi

Svaka stavka grafika prikazuje koliko puta je sličan odgovor dat i u anketi i u okviru eksperimenta. Kao što se i na grafiku vidi, najčešći razlozi uključuju naviku korišćenja QR kodova, a pogotovo kada je riječ o mogućnosti da se nekome pomogne ljudi su osjetljivi.

Anketom je utvrđeno da je manje od 50% učesnika ankete imalo priliku da učestvuje u nekoj obuci ili treningu na temu sajber bezbjednosti kao i da je manje od 50% učesnika svjesno da postoji rizik pri skeniranju QR kodova. Učesnici ankete svojim odgovorima pokazali su da se ovakvo znanje manifestuje rizičnim ponašanjem kada je u pitanju sigurno skeniranje QR kodova i akcije na koje QR kodovi mogu da pozivaju poput ostavljanja ličnih podataka ili preuzimanja aplikacija sa neprovjerenih sajtova, pa je samo 8% od ukupnog broja učesnika izjavilo da je preduzelo mjeru sigurnosti pri skeniranju QR koda a oko 20% njih pokazalo rizično ponašanje nakon skeniranja. Eksperimentom kojim je potpuno nepoznat QR kod skeniralo 88 slučajnih učesnika eksperimenta za kratak vremenski perios i odgovorima da se QR kodovi koriste bez previše razmišljanja (odgovor koji su uglavnom davali i učesnici ankete), pokazuje da je rizik od fišing napada putem QR kodova u Crnoj Gori realan a uzimajući u obzir rezultate koji su u anketi postigli učesnici iz IT oblasti zanimanja a koji su odgovorili pozitivno na pitanje o obuci iz sajber bezbjednosti, edukacija se predstavlja kao najefikasnije rješenje problema.

Zaključak

QR kodovi su postali izuzetno popularni zbog svoje jednostavnosti i efikasnosti kada je riječ o prenosu informacija. Međutim, zbog svoje popularnosti postali su sredstvo različitim vrstama napada pogotovo fišing napada. Rezultati ankete sprovedene u okviru rada pokazuju da većina korisnika nije dovoljno svjesna bezbjednosnih rizika povezanih sa skeniranjem QR koda i većina ne preduzima nikakve mjere opreza, prije nego što skenira neki QR kod, što ih čini lakim metama.

Fišing napadi koji se izvode putem QR kodova predstavljaju ozbiljnu prijetnju jer mogu preusmjeriti korisnike na zlonamjerne web stranice koje izgledaju legitimno i na taj način od korisnika ukrasti osjetljive podatke. Eksperimentalni dio rada, takođe, je dodatno potvrdio da korisnici mogu biti veoma lako prevareni kada dođe do skeniranja samog koda i potvrdio je potrebu za povećanjem svijesti korisnika o bezbjednosnim praksama.

Rad ukazuje na hitnu potrebu za podizanjem svijesti o bezbjednosnim rizicima povezanim sa QR kodovima, ali i o bezbjednosti na Internetu uopšte, te veliku potrebu za implementacijom sigurnosnih mjera koje su neophodne svima u sajber prostoru. Za buduća istraživanja ostavljena je anketa i ekperiment koji je izvršen u okviru rada kao i rezultati istih.

Anketnim istraživanjem zaključeno je da iako većina korisnika koristi QR kodove u svakodnevnom životu (više od 94% od ukupnog broja učesnika), manje od pola (46%) je svjesno rizika koji korišćenje istih nosi a tek nešto više od 8% od ukupnog broja učesnika ankete preduzima dodatne sigurnosne mjere prilikom skeniranja istih.

Podaci dobijeni anketnim istraživanjem poklopili su se sa podacima dobijenim eksperimentom u kome je na jednostavnu poruku da se skenira QR kod kako bi ostvarilo učešće u humanitarnoj akciji "nasjelo" 88 slučajnih korisnika a većina koja je pristala da učestvuje dalje u eksperimentu je dala odgovor da nesmotreno skenira QR kodove ne očekujući da to može imati negativan uticaj ili potencijalnu opasnost.

Rezultati dobijeni u radu ukazuju da su određene grupe ranjivije od drugih kada je bezbjednost pri skeniranju QR kodova u pitanju, te da ove grupe mogu biti predmet budućnih istraživanja na temu kao i ciljna grupa u edukacionim radionicama.

Literatura

[1] Narayanan, A.S. „QR Codes and Security Solutions“. International Journal of Computer Science and Telecommunications 3(7) 69-71, 2012.

[2] Banu, M. N., & Banu, S. M. „A Comprehensive Study of Phishing Attacks“ International Journal of Computer Science and Information Technologies, 4(6), 783, 2013.

[3] Dr. Rammanohar Lohia: „QR Code Generator: A Security Perspective“, Avadh University, Ayodhya, India 01- 55, 2022

[4] J. Rouillard: „Contextual QR codes“, in Proc. IEEE 3rd Int. Multi Conf.Comput. Global Inf. Technol. (ICCGI), 2008, pp. 50–55

[5] Tina Z˘ urbi1 and Diana Gregor-Svetec:„Use of QR Code in Dairy Sector in Slovenia“, 1-16, 2023.

[6] Alnajjar, A. Y., Manickam, S., Anbar, M., Al-saleem, S. and Elejla, O.. TrustQR: „A New Technique for the Detection of Phishing Attacks on QR Code“. Advanced Science Letters, 22 (10), 2905–2909, 2016.

[7] Bilir M. O. and Erguner Özkoc, E.:“A research on the QR code security awareness in Ankara“ Journal of Internet Applications & Management, 1-11, 2020.

[8] A. Patel, A. Joseph, S. Survase, and R. Nair, “Smart student attendance system using QR code,” SSRN Electronic Journal, 2019, 1-4

[9] Smartphone Users Around the World – Statistics and Facts, http://www.go-gulf.com/blog/smartphone/

[10] Kapsalis, I., Security of QR Codes. Norwegian University of Science and Technology, Norway, 2013, 5-18

[11] T. Vidas, E. Owusu, S. Wang, C. Zeng, L. Cranor. QRishing: „The susceptibility of smartphone users to QR code phishing attacks.“ CMU-CyLab-12 pp. 1–12., 2012.

[12] Y. Zhang, J. Hong, L. Cranor. Cantina: „A content-based approach to detecting phishing web sites.“ ,Proceedings of the 16th international conference on World Wide Web, WWW ’07, 1-10, 2007.

[13]Kevin Peng, Harry Sanabria, Derek Wu, Charlotte Zhu: "Security owerview of QR codes", Massachusetts Institute of Technology, 2014, 3-20.

[14]Zainab Alkhalil, Chaminda Hewage *, Liqaa Nawaf and Imtiaz Khan: „Phishing Attacks: A Recent Comprehensive Study and a New Anatomy“, Cardiff School of Technologies, Cardiff Metropolian University, Cardiff, Unighted Kingdom, 2021, 3-19.

[15]Samuel M. Kori, „Analysis of Security Issues with QR Codes“, Faculty of Science and Technology, Bournemouth University, 2022, 11-20.

[16]Sumit Tiwari, Madhya Pradesh, “An Introduction to QR Code Technology”, International Conference on Information Technology, 2016, 39-44.

[17]Dr Girisha H1 , A Dheerendra Kumar2 , Atithi Singh3 , Bharath K P4 , Deepa, ‘’QR Code Detection’,’ International Journal of Advanced Research in Science, Communication and Technology (IJARSCT) Volume 2, Issue 9, June 2022.

[18]Majdi Msallam, ‘’Bar codes techniques’’, Higher Institute for Applied Sciences and Technology, 1-22, 2013.

[19]Lana Sotnik, ‘’MANUFACTURING & MECHATRONIC SYSTEMS’’ VII International Conference, 5-12, 2023.

[20]Riyadh Rahef Nuiaa, ‘’ A Critical Review: Revisiting Phishing Attacks Classification and Analysis of Techniques Employed in Taxonomies’’, Wasit Journal for Pure Sciences Vol. (2) No. (2), 2023.

[21]"QR code development story", QR Code development story | Technologies | DENSO WAVE (denso-wave.com)

[22]Y Alta Van der Merwe, "Characteristics and responsibilities involved in a Phishing attack", University of Pretoria, January 2005

[23] NC. Filipo Sharevski, Mattia Mossano, Ghunter Schiefer, "Exploring Phishing Threats through QR Codes in Naturalistic Settings", Conference: Symposium on Usable Security and Privacy (USEC) 2024At: San Diego, California, February 2024.

[24]Marvin Peter Schimid, "A QR code phishing prevention system", *University of Castilla-La Manchai*, March 2022, 23-24.

[25]Nidhi Prasad, Sanay Kumar, "Survey research – concept and development", *Jurnal of Indira Gandhi Institute of Medical Sciences,* 2024, 2-6.

[26]Marco Palmieri, Rosario Aprile, "Data quality in Social Surver Research", *Encyclopedia of Information Science and Technology,* 2024, 1-13.

[27]"How to use QR codes safely", *Government of Canada, 2022,* How to use QR codes safely - Get Cyber Safe

[28]"QR codes – what's the real risk?", *National Cyber Security Center of Great Britain,* QR Codes - what's the real risk? - NCSC.GOV.UK, 2023.

[29]"Skriveni rizici upotrebe QR kodova", Vlada Crne Gore, Skriveni rizici upotrebe QR kodova (www.gov.me), 2023.

[30]Godwin Awuah Amoah, Hayfron-Acquah J.B., "QR Code Security: Mitigating the Issue of Quishing (QR Code Phishing)", *International Journal of Computer Applications,* October 2022. 2-7.

Dodatak 1.

Prvi dio – opšte informacije

1. Starosna dob
   - 1-18
   - 18-25
   - 25-40
   - 40-60
   - 60+

2. Pol
   - Muški
   - Ženski

3. Posljednji završeni nivo obrazovanja
   - Osnovna škola
   - Srednja škola
   - Viša škola
   - Fakultet/Osnovne studije
   - Specijalističke studije
   - Master studije
   - Doktorske studije

4. Oblast zanimanja
   - Prirodne nauke
   - Društvene nauke
   - Tehničke nauke

5. Ukoliko je Vaš odgovor na pitanje broj 5. Bilo “Tehničke nauke”, da li se radi o nekoj od oblasti informacionih tehnologija?
    - Da
    - Ne

Drugi dio ankete – opšta informisanost o QR kodovima

6. Da li znate šta su QR kodovi?
    - Da
    - Ne

7. Da li ste imali priliku da skenirate neki QR kod u posljednjih 10 dana?
    - Da
    - Ne

Treći dio – opšta informisanost o sajber bezbjednosti i fišing napadima

8. Da li ste upoznati sa činjenicom da postoji opasnost na Internetu?
    - Da
    - Ne

9. Da li ste upoznati sa pojmom fišing napad?
    - Da
    - Ne

10. Ukoliko je na prethodno pitanje Vaš odgovor "Da", da li možete objasniti ili dati primjer fišing napada?

11. Da li ste imali priliku da budete “žrtva” fišing napada?
    - Da
    - Ne

12. Ukoliko je na prethodno pitanje Vaš odgovor "Da", da li možete napisati na koji način je izvršen napad, putem elektronske pošte, društvenih mreža, SMS poruke ili nešto drugo?

13. Da li smatrate da ste dovoljno informisani o rizicima koji postoje u sajber prostoru?
    - Da
    - Ne

14. Da li ste nekada u privatnom ili poslovnom životu imali priliku da prisustvujete nekom treningu ili obuci o važnosti sigurnosti na Internetu?
    - Da
    - Ne

Peti dio - Bezbjednosni rizici skeniranja QR kodova

15. Da li ste upoznati da postoje bezbjednosni rizici skeniranjem QR kodova?
    - Da
    - Ne

16. Da li ste imali priliku da se susretnete sa QR kodom nakon čijeg skeniranja ste pozvani na neku akciju: registraciona forma, preuzimanje fajla ili neka aplikacije ili slično?

    - Da
    - Ne

17. Da li ste ikada, nakon što ste skenirali QR kod preuzeli neku aplikaciju sa neprovjerene lokacije (a da to nije Play store/App store)

    - Da
    - Ne

18. Da li ste nekada preduzeli neku dodatnu mjeru prije nego što ste skenirali QR kod?
    - Da
    - Ne

19. Ukoliko je vaš odgovor na prethodno pitanje bio "DA", da li nam možete reći o kojoj provjeri je riječ? (provjera na web stranici, poziv na broj telefona itd)
20. Dodatni komentar, sugestija, kritika?