SMIŠING I RAZVOJ SMS PREVARA

Savremeni rizici i mere zaštite

REPUBLIKA SRBIJA
RATEL
REGULATORNO TELO ZA ELEKTRONSKE KOMUNIKACIJE I POŠTANSKE USLUGE

SRB-CERT

www.cert.rs

Nacionalni CERT Republike Srbije

Decembar 2025

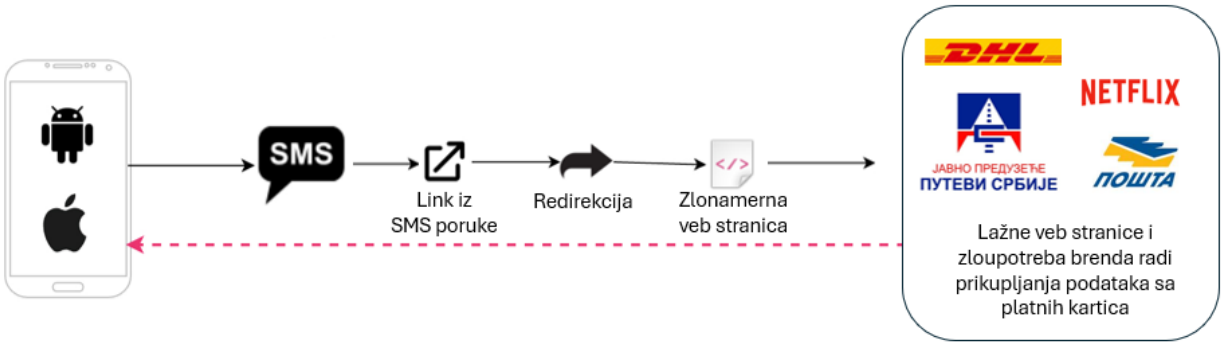
Uvod

Prva SMS poruka poslata je 3. decembra 1992. godine, kada je britanski inženjer Nil Papvort sa računara preko mreže „Vodafone GSM“ uputio svom kolegi poruku „Srećan Božić“. Od tog trenutka SMS je postao simbol brze i direktne komunikacije, ali ubrzo i sredstvo koje su napadači počeli da zloupotrebljavaju.

Sve veći broj prevara odvija se putem SMS poruka, koje deluju kao zvanična obaveštenja od banke, kurirske službe, državne institucije, mobilnog operatora, poznatih digitalnih platformi kao što su Netflix, Spotify i drugi striming ili platni servisi. One mogu sadržati zlonamerne linkove, zahteve za lične podatke, podatke o platnoj kartici ili uputstva koja korisnika dovode u rizik od prevare i gubitka novca.

Smišing (SMS fišing) predstavlja oblik digitalne prevare u kom prevaranti šalju SMS poruke koje izgledaju kao zvanična obaveštenja, sa ciljem da navedu korisnika da otkrije lične podatke, podatke sa platne kartice ili da klikne na zlonamerni link.

U 2024. godini Nacionalnom CERT-u građani su prijavili SMS prevare i ukupan finansijski gubitak u iznosu od približno dva miliona dinara. Statistika kojom raspolaže Nacionalni CERT zasniva se na prijavljenim slučajevima SMS prevara, pa je važno napomenuti da mnoge žrtve prevara nisu prijavile prevaru, ali ni iznos finansijskog gubitka, što znači da je stvarna šteta znatno veća od evidentirane. U toku 2024. godine sve SMS prevare su bile usmerene na korisnike poštanskih usluga.



Slika 1 - Put od SMS poruke do krađe podataka

Prvi pokušaji smišinga

U početnim godinama mobilne telefonije, SMS prevare su bile prilično jednostavne. Najčešće su se svodile na to da korisnik pozove broj sa visokom tarifom ili uplati pripejd kredit na tuđi račun. Iako su takve poruke vremenom postale lako prepoznatljive, i dalje se koriste kao metod obmane.

Primeri poruka:

- „Osvojili ste nagradu, javite se na broj…“
- „Ćao pišem ti sa novog broja, molim te uplati mi dopunu pripejd kredita za ovaj broj…“
- „Mama pozovi me na ovaj broj, izgubio sam telefon…”

Psihološki pritisak kao napredna taktika: hitnost i strah

U poslednjih nekoliko godina, SMS prevare su se transformisale u smišing kampanje. Korisnici su postajali sve svesniji prevara, pa su prevaranti počeli da kombinuju taktike hitnosti i straha. Razvili su se automatizovani sistemi za slanje poruka velikom broju korisnika. Poruke dolaze sa brojeva koji izgledaju kao da su zvanični, a likovi vode ka uverljivim veb sajtovima koji koriste moderan dizajn.

Ove poruke sadrže linkove ka lažnim sajtovima koji izgledaju kao stranice banaka, pošte ili državnih institucija. Često imitiraju stil i sadržaj banke, kurirske službe, državne institucije, mobilne operatore ili imitiraju izgled poznatih platformi kao što su Netflix, Sportify i slično.

U porukama se nalaze hitni pozivi na akciju, a to kod korisnika izaziva paniku i brzu reakciju.

Primeri poruka:

- „Zabeležen je Vaš saobraćajni prekršaj, kliknite na link da biste platili kaznu“
- „Vaš paket je zadržan. Platite 150 din za carinjenje da biste dobili paket: [link]“
- „Banka: vaš nalog je privremeno blokiran. Prijavite se ovde da biste mogli da nastavite da koristite usluge banke: [link]“
- „Netflix pretplata nije produžena. Potvrdite karticu ovde: [link]“

Tehnološki napredak: Zloupotreba identiteta pošiljaoca i smišing kampanje

Sa porastom svesti građana o SMS prevarama i zlonamerni akteri usavršavaju svoje metode. Jedna od najopasnijih taktika je zloupotreba identiteta pošiljaoca, gde poruka izgleda kao da dolazi od zvanične institucije, banke, mobilnog operatora ili poznate platforme – iako to nije slučaj.

Tehnika koja se primenjuje u SMS prevarama, u kojoj napadač falsifikuje identitet pošiljaoca poruke kako bi prevario primaoca, naziva se **SMS spufing** (engl. SMS spoofing).

Zašto je ova taktika opasna?

- Korisnik često ne proverava pošiljaoca ako prepozna ime,
- Poruka izgleda legitimno i ne sadrži očigledne greške,
- Link vodi ka stranici koja vizuelno podseća na zvaničnu platformu.

Kako se sprovodi ova napredna SMS prevara?

U svetu mobilne komunikacije, važno je razumeti razliku između P2P (Person-to-Person) i A2P (Application-to-Person) poruka, jer upravo ova razlika igra ključnu ulogu u razumevanju kako se zloupotrebljavaju SMS poruke i nastaju SMS prevare.

P2P – Poruke između dve osobe

P2P komunikacija podrazumeva razmenu SMS poruka između dva fizička lica. To su klasične poruke koje šaljemo prijateljima, porodici ili kolegama.

Karakteristike:

- Poruke se šalju sa mobilnog broja na mobilni broj,
- Ne koristi se kod masovne distribucije,
- Ne koriste automatizovane sisteme,
- Uglavnom nisu predmet zloupotrebe u kontekstu SMS prevara.

A2P – Poruke od aplikacija ka korisnicima

A2P komunikacija podrazumeva poruke koje se šalju od strane aplikacija u ime banaka, institucija ili platformi ka korisnicima. To su poruke koje dobijamo kao obaveštenja, potvrde, kodove za prijavu ili potvrdu, podsetnike i slično.

Karakteristike:

- Poruke se šalju sa sistemskih brojeva ili alfanumeričkih pošiljalaca (npr. „Netflix“, banka, Pošta Srbije),
- Često koriste automatizovane sisteme za masovnu distribuciju,
- Mogu sadržati linkove, kodove, pozive na određene aktivnosti,
- Ovo je način komunikacije koji prevaranti zloupotrebljavaju – imitirajući zvanične pošiljaoce i sadržaj.

Zašto je važno razlikovati?

Poruke koje izgledaju kao A2P, ali dolaze od prevaranata, mogu lako da navedu korisnika da klikne na link, unese podatke ili izvrši uplatu. Zato je važno da građani znaju da:

- Zvanične institucije retko traže lične podatke putem SMS-a,
- Pošiljalac se može lažno prikazati kao zvaničan,
- Lažne A2P poruke se često koriste u smišing kampanjama.

Za A2P komunikacije postoje aplikacije uz pomoć kojih može da se unese bilo koji tekst, broj ili njihova kombinacija u polje za identifikaciju pošiljaoca, to je alfanumerički naziv odnosno „Sender ID“.

Karakteristike:

- Ubacivanje lažnih poruka u postojeći niz,
- Manipulacija Sender ID-om,
- Tehnike koje koriste kontekst i vreme (npr. nakon prave poruke od kurirske službe).

Primeri:

- Lažni naziv pošiljaoca (Sender ID): Umesto broja, poruka se prikazuje kao da je stigla od Pošte Srbije, banke, od NETFLIX-a ili operatora, što kod korisnika izaziva poverenje,
- Ubacivanje u postojeći niz poruka: Zlonamerni akteri ponekad uspeju da poruka izgleda kao deo prethodne komunikacije sa institucijom, što dodatno otežava prepoznavanje prevare,
- Izgled poruke: Formulacije, pravopis i vizuelni stil poruke imitiraju zvanične šablone, uključujući logoe, potpise i linkove koji liče na prave adrese.

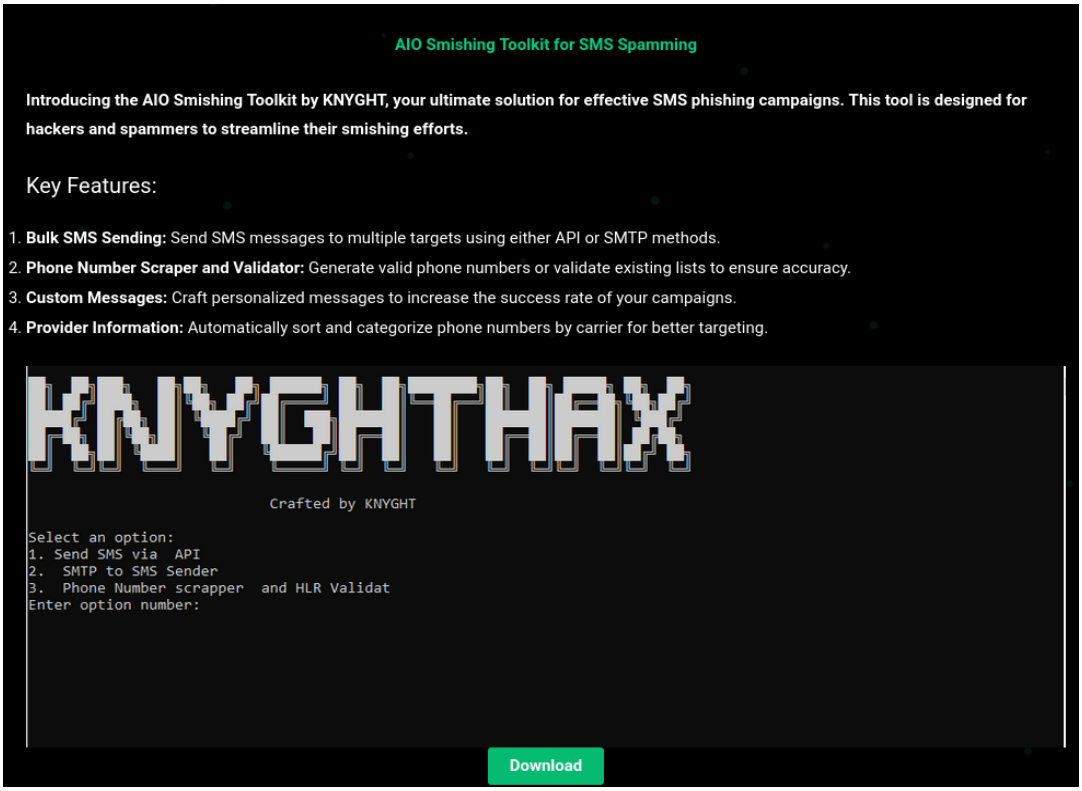
AIO (all-in-one) softverski alati za smišing napade

Napadači koriste specijalizovane alate AIO (all-in-one) za automatizovane smišing napade koji omogućavaju masovno slanje lažnih SMS poruka i krađu podataka uz minimalan trud. Ovi alati kombinuju više funkcija u jednoj platformi, čineći ih izuzetno efikasnim i opasnim. Omogućavaju automatizaciju napada i masovno slanje lažnih SMS poruka korisnicima širom sveta, lažno predstavljanje kao banke, kurirske službe, državne institucije uz adekvatan prevod na jezik korisnika.

Primer alata za smišing, poznat kao „AIO Smishing Toolkit“, prikazan je na Slici br. 2. Ovaj softverski paket omogućava napadaču da:

- masovno šalje SMS poruke na više brojeva, koristeći različite tehničke metode
- proveri da li su brojevi telefona aktivni i važeći, čime se izbegavaju neuspešne isporuke,
- formuliše personalizovane poruke radi povećanja uverljivosti i efikasnosti napada,
- sortira i kategorizuje listu brojeva prema mobilnom operatoru, što omogućava preciznije targetiranje žrtava.

Ovakvi alati pokazuju koliko su današnje SMS prevare tehnički napredne i zašto je važno da građani budu informisani i oprezni.



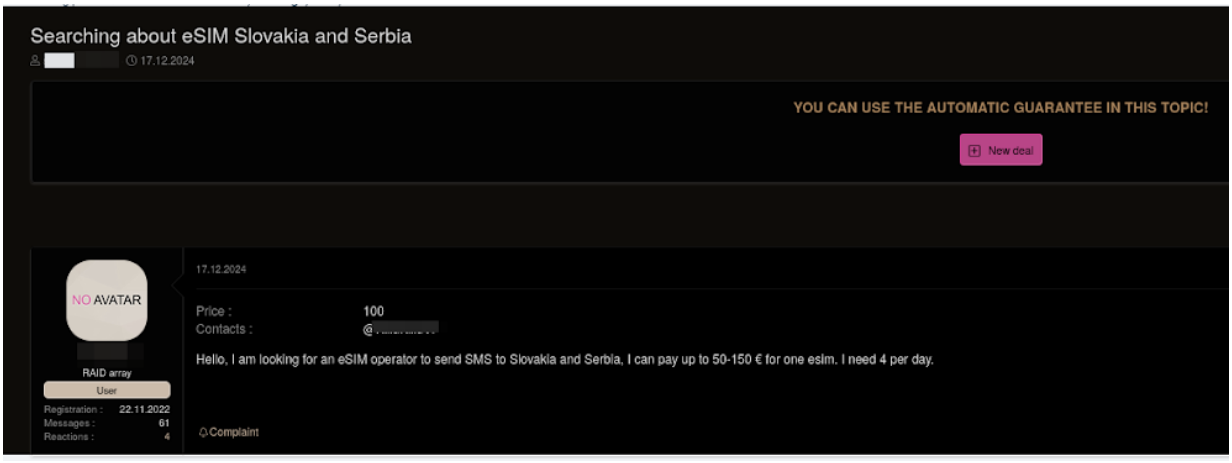
Slika 2 - Alat za realizaciju smišing napada

Napadači dolaze do brojeva telefona putem različitih izvora, često nelegalnih, koji im omogućavaju da masovno šalju smišing poruke. Baze podataka koje sadrže podatke građana najčešće kupuju na crnom tržištu.

Te baze potiču iz:

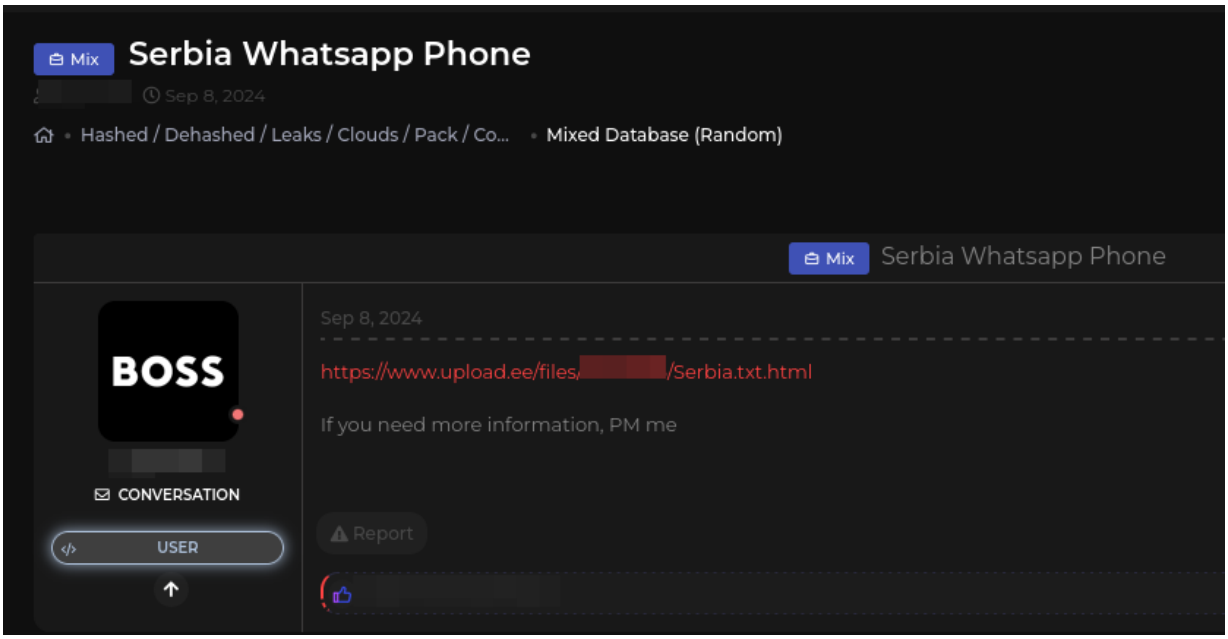
- ukradenih podataka sa platformi za e-trgovinu, na kojima građani ostavljaju podatke,
- nezaštićenih onlajn formulara,
- putem aplikacija koje traže dozvolu za pristup kontaktima na mobilnom telefonu,
- iz javnih izvora (oglasi, društvene mreže, forumi gde korisnici ostavljaju kontakt).

Na slici br. 3 prikazana je forumska poruka sa dark veba, u kojoj korisnik traži eSIM kartice za slanje SMS poruka ka Srbiji. Post je objavljen 17. decembra 2024. godine, a korisnik je registrovan krajem novembra 2022. godine. U poruci se navodi da je spreman da plati 50 do 150 evra po jednoj eSIM kartici, da mu je potrebno četiri kartice dnevno i da želi da šalje SMS poruke ka navedenim državama. Ova slika ukazuje na postojanje tržišta, na forumima koji nisu javni ili zvanični, za nabavku eSIM resursa u svrhu masovnog slanja SMS poruka, što može biti povezano sa smišing kampanjama ili drugim oblicima zloupotrebe mobilnih komunikacija.



Slika 3 - Forumska poruka sa dark veba

Na slici br. 4 je primer forumske razmene podataka i brojeva mobilnih telefona koji mogu biti zloupotrebljeni u smišing kampanjama. Prikazan je post sa onlajn foruma pod nazivom „Serbia Whatsapp Phone“, u okviru kategorije „Mixed Database [Random]“. Post je objavljen 8. septembra 2024. godine. U sadržaju poruke nalazi se link ka datoteci pod nazivom „Serbia.txt.html“, koja je hostovana na spoljnjoj platformi za deljenje fajlova. Opis teme i oznake („Hashed / Dehashed / Leaks / Clouds / Pack…“) ukazuju da se radi o potencijalno kompromitovanim podacima, verovatno telefonskim brojevima povezanim sa WhatsApp korisnicima u Srbiji. Ovo je i primer kako se lični podaci mogu naći na dark webu i zašto je važno da građani budu oprezni sa deljenjem broja telefona i aktivnostima na mobilnim aplikacijama.



Slika 4 - Primer objave sa dark veba: deljenje liste brojeva iz Srbije

Nova generacija SMS prevara: Poruke koje se nastavljaju na legitimne u istom nizu

Savremene SMS prevare više ne izgledaju kao poruke od nepoznatih brojeva sa lošim pravopisom. Naprotiv, prevaranti koriste tehnički napredne metode koje poruke čine uverljivim, vremenski usklađenim i vizuelno identičnim zvaničnim obaveštenjima.

Jedna od najopasnijih taktika je ubacivanje lažne poruke u postojeću prepisku sa bankom, kurirskom službom ili mobilnim operaterom. Korisnik vidi poruku u istom nizu kao prethodne zvanične poruke, što stvara utisak da je i nova poruka pouzdana.

Korisnici često imaju naviku da veruju porukama koje stižu u već postojeće prepiske sa institucijama, pa je ovaj oblik napada posebno opasan. Zbog toga je važno da se uvek proveri sadržaj poruke, da se ne pristupa sumnjivim linkovima, kao i da se informacije potvrde direktno preko zvaničnih aplikacija ili internet stranica.

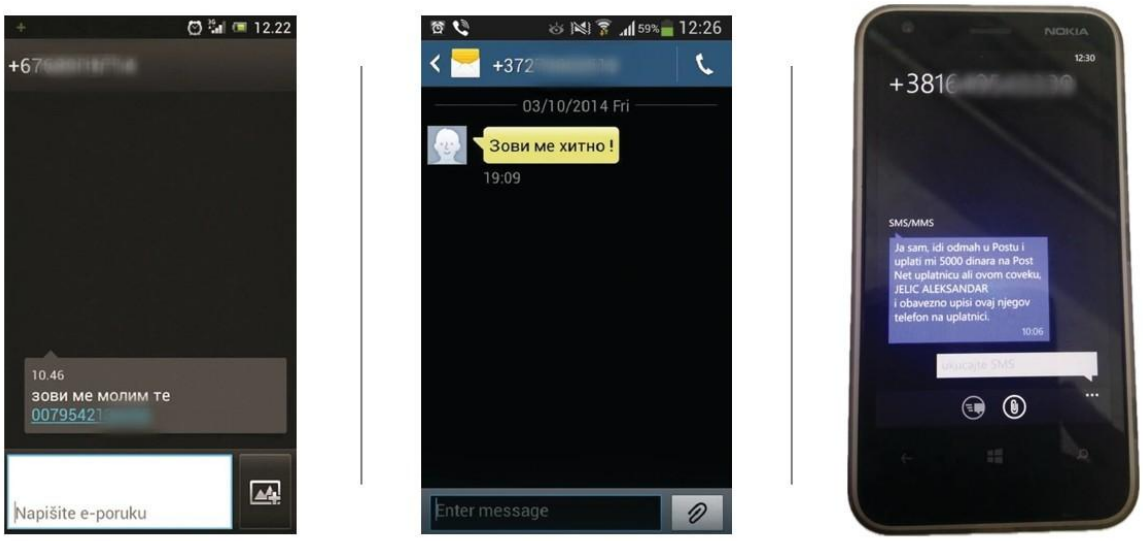
Napadači to postižu tako što namerno manipulišu poljem Sender ID. U praksi, oni najčešće zloupotrebljavaju slabo zaštićene SMS gateway-e i A2P aplikacije u kojima mogu da podese identifikator pošiljaoca po želji. Na taj način poruka izgleda kao da je stigla od banke ili druge institucije. Mobilni telefoni sve poruke grupišu upravo po tom identifikatoru, pa sistem ne pravi razliku između legitimne i lažne poruke ako obe nose isti Sender ID. Na taj način, korisnička aplikacija u mobilnim telefonima prikazuje sve poruke u jednom nizu, što prevaru čini uverljivom i teškom za prepoznavanje.

Ređi i tehnički složeniji slučaj je zloupotreba SS7 protokola koji omogućava razmenu signalizacionih poruka između mobilnih mreža.

Primeri SMS prevara

Prvi pokušaji smišinga

Klasične SMS prevare imaju primaran cilj da navedu primaoca da reaguje: da odgovori, pozove broj ili da sledi instrukcije koje dovode do finansijskog gubitka. Poruke obično stižu sa nepoznatih brojeva i sadrže lažne, ali uverljive informacije.



Slika 5 - Primeri klasičnih SMS prevara

Važno je ostati oprezan i ne reagovati impulsivno na poruke koje deluju hitno ili neobično. Treba uvek prvo razmisliti o sadržaju poruke pre preduzimanja bilo kakve akcije.

Pošta Srbije

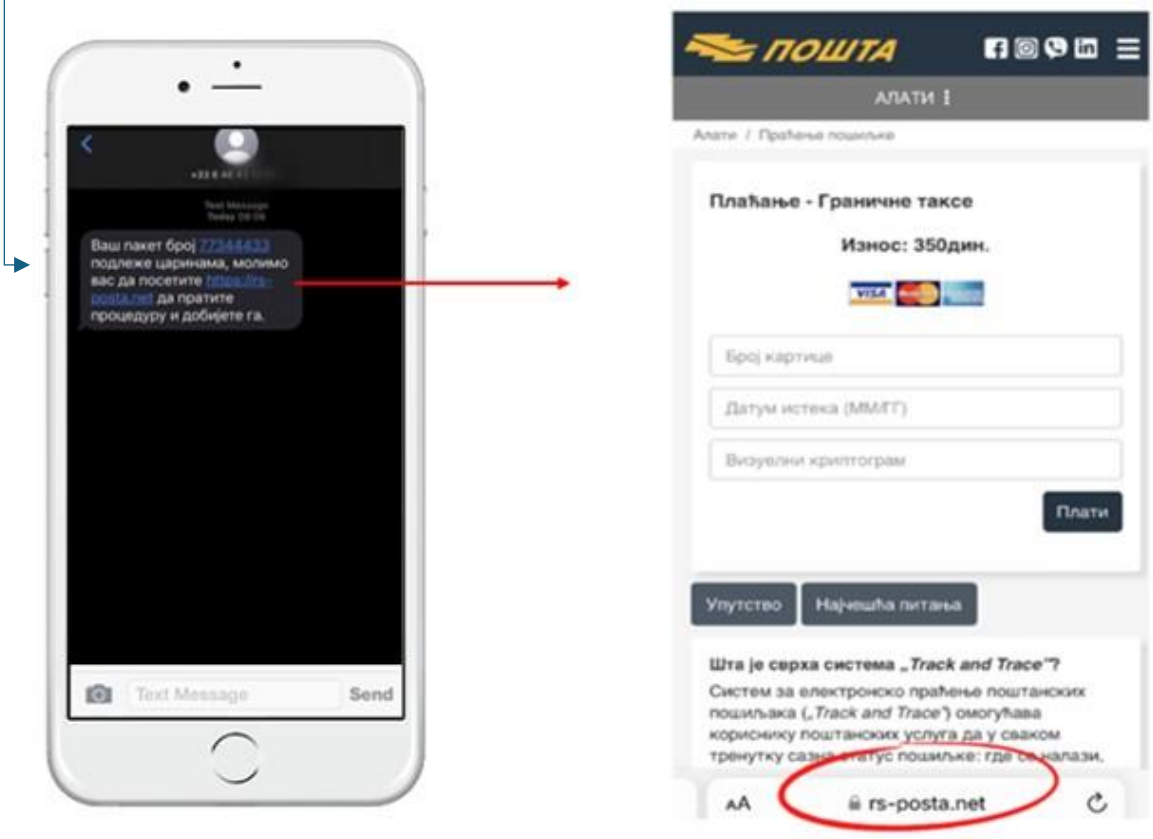
Korisnicima se šalje lažna SMS poruka da im navodno paket nije mogao biti isporučen zbog neplaćene carine i da za isporuku treba otvoriti link iz poruke.

Primeri lažnih linkova:
https://rs-posta.com
https://rs-posta.net
https://posta-serbia.com
https://posta-srbija.com

Legitiman link:
https://www.posta.rs/

Ваш пакет број 77344433 подлеже царинама, молимо вас да посетите

https://rs-posta.net да пратите процедуру и добијете га

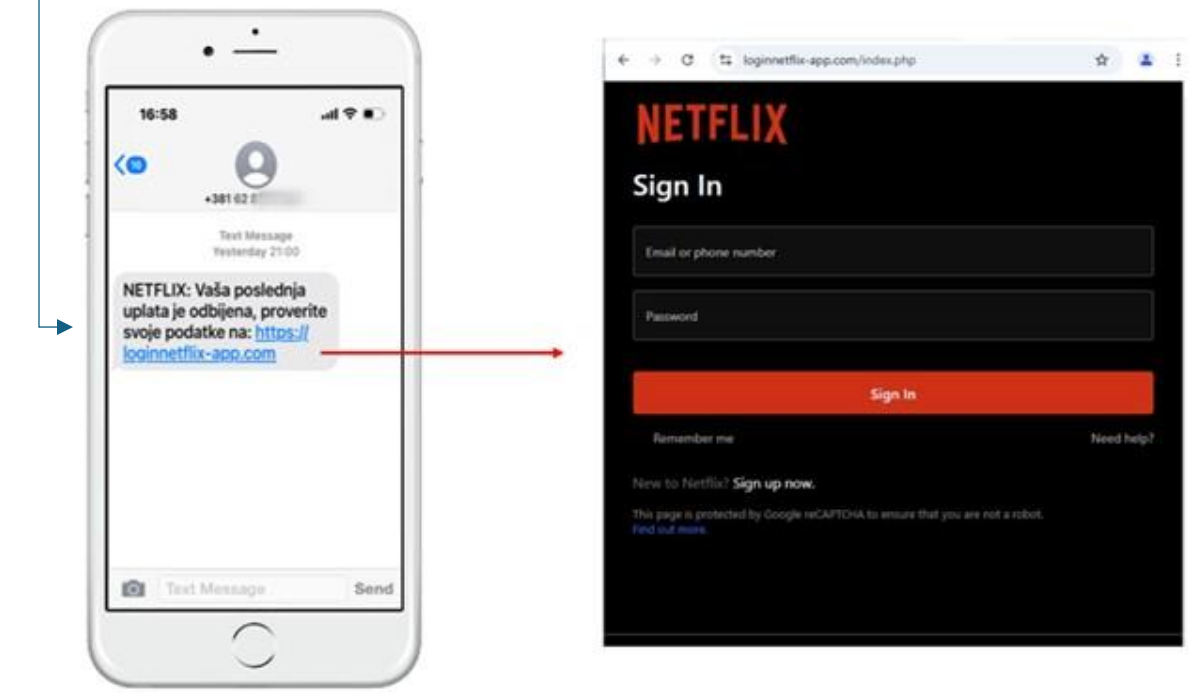


Slika 6 - Prevara koja se odnosi na Poštu Srbije

Netflix prevara

Prevaranti šalju poruku koja izgleda kao obaveštenje od Netflix-a, a link vodi ka lažnoj stranici za prijavu. Unosom podataka, korisnik nesvesno otkriva svoje poverljive informacije.

NETFLIX: Vaša poslednja uplata je odbijena. Proverite svoje podatke na: https://loginnetflix-app.com



Slika 7 - Prevara koja se odnosi na Netflix

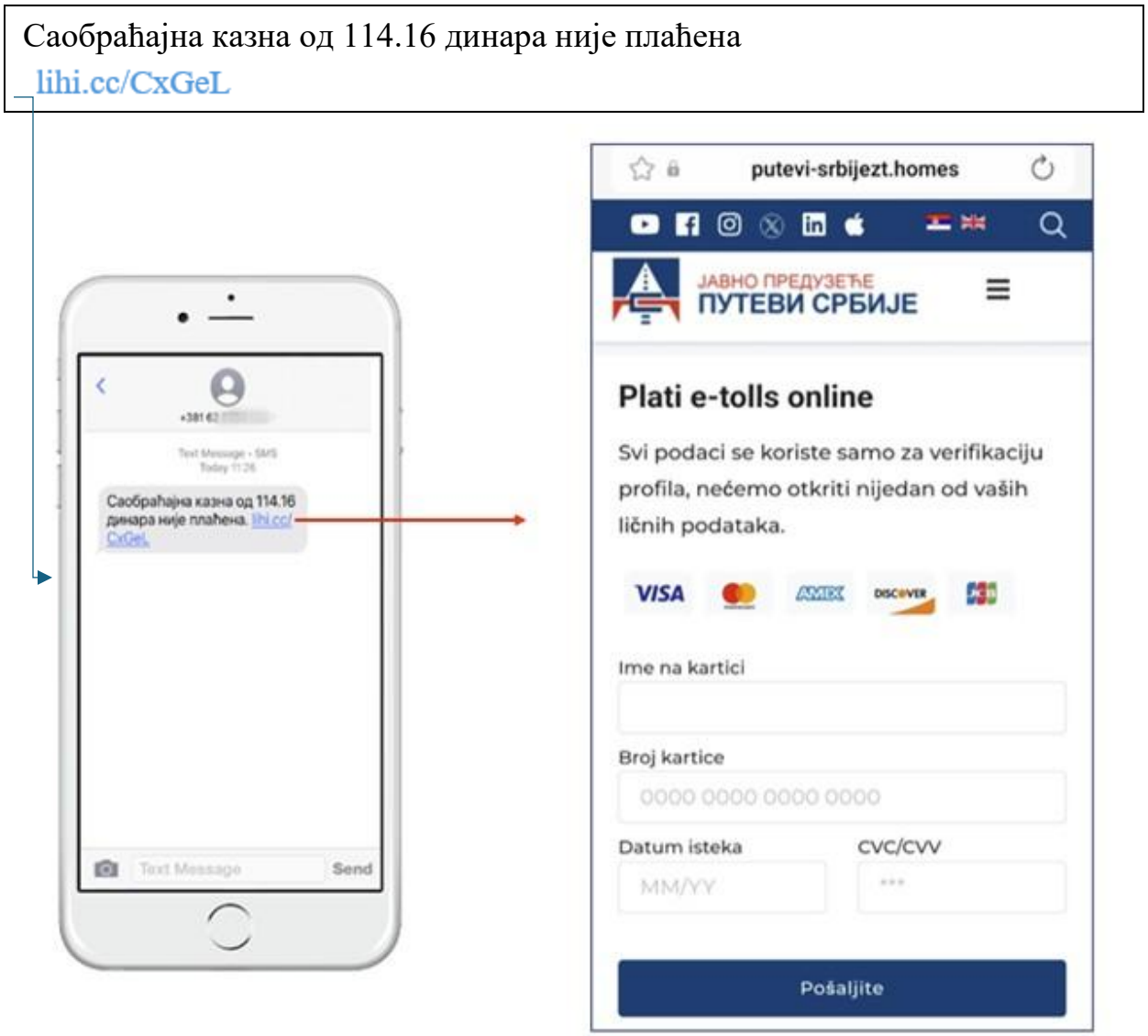
Šta ovaj primer pokazuje:

- SMS poruka: izgleda zvanično ali sadrži poziv na akciju i link koji nije zvaničan,
- Lažna stranica: imitira Netflix, ali URL nije zvaničan,

  (npr. *https://loginnetflix-app.com* umesto zvaničnog *https://www.netflix.com*),
- Rizik: unosom podataka, korisnik omogućava pristup nalogu ili podacima sa platne kartice.

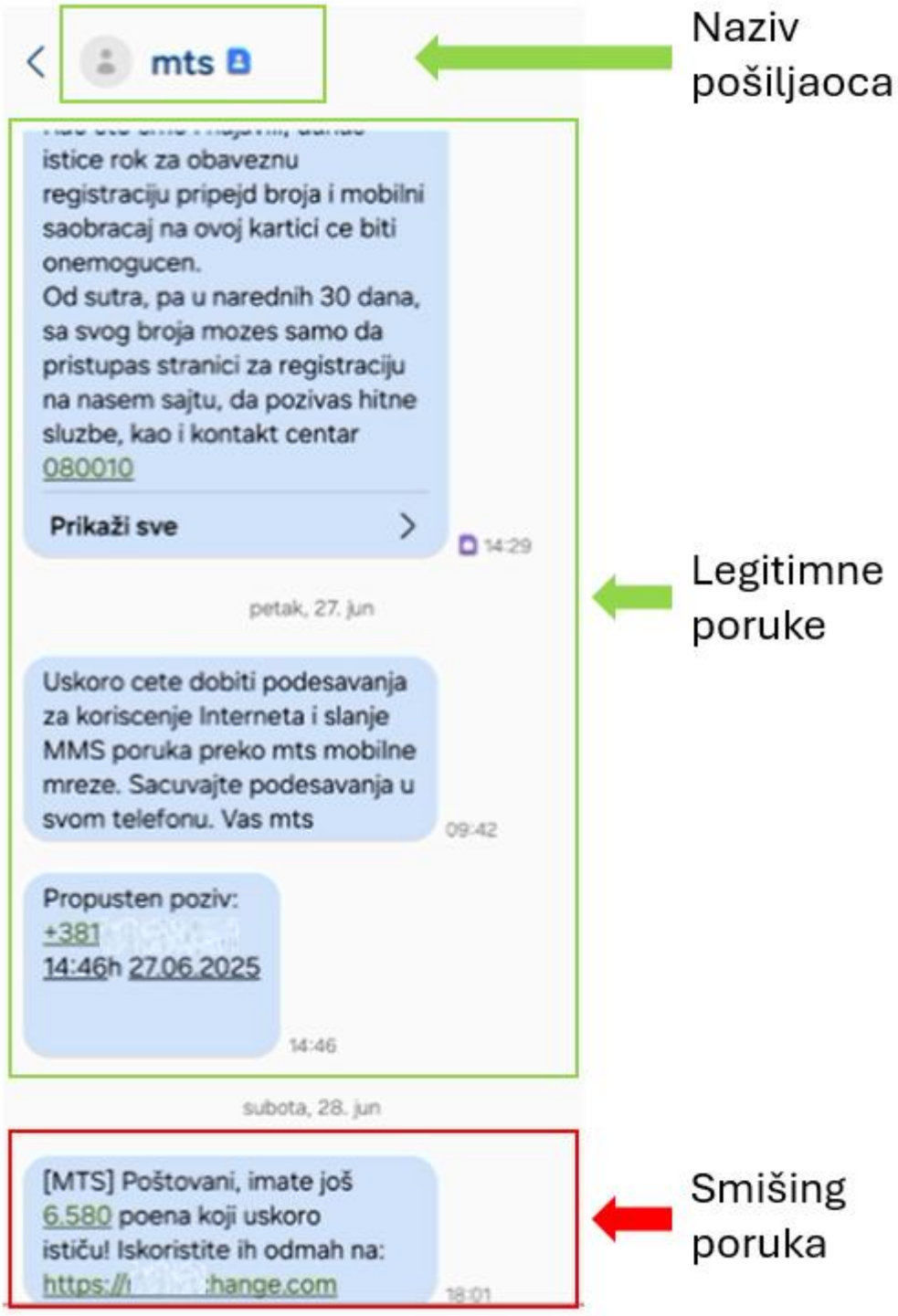
Putevi Srbije

U smišing kampanji koja je usmerena na Puteve Srbije, napadač se lažno predstavlja kao „JP Putevi Srbije“. U tim porukama se navodi da je primalac načinio saobraćajni prekršaj ili nije platio putarinu, uz poziv da preko priloženog linka izvrši uplatu. Link vodi ka lažnoj internet stranici koja oponaša zvaničnu instituciju, a krajnji cilj je da se građani navedu da unesu podatke sa svoje platne kartice, čime se omogućava zloupotreba, odnosno krađa novca.



Slika 8 - Prevara koja se odnosi na Puteve Srbije

Primer prevare putem SMS poruke koja se pojavljuje u legitimnom nizu poruka



Slika 9 - Smišing poruke koje se nastavljaju u istom nizu na legitimne

Od ključne je važnosti da korisnik ne reaguje impulsivno. Pre bilo kakve akcije, potrebno je pažljivo proveriti ko je pošiljalac i šta poruka zaista sadrži. Samo oprezom i kritičkim razmišljanjem možemo se zaštititi od ovakvih obmana.

Mere zaštite

Obazrivo pristupajte porukama koje traže hitnu akciju

- Ako se u poruci tvrdi da morate odmah da kliknete na link, platite kaznu, potvrdite identitet ili unesete adresu za dostavu paketa – budite sumnjičavi.

Preporučuje se oprez pri pristupu sumnjivim linkovima

- Linkovi u porukama mogu voditi ka lažnim sajtovima koji izgledaju kao banke, pošte ili kurirske službe,
- Umesto klika otvorite zvaničnu veb stranicu ili pozovite kontakt centar.

Izbegavajte unos ličnih podataka putem SMS-a

- Proverite da li je pošiljalac zaista zvaničan – institucije retko šalju linkove putem SMS-a,
- Banke, državne institucije i kurirske službe nikada neće tražiti PIN, lozinku ili podatke sa platne kartice putem poruke,
- Ne unosite podatke preko linkova iz poruka, već direktno preko zvaničnog sajta.

Koristite aplikacije za zaštitu mobilnih uređaja

- Aktivirajte opcije za blokiranje ili filtriranje nepoznatih pošiljalaca,
- Ako ste u mogućnosti instalirajte verziju antivirusne aplikacije koja ima zaštitu od smišing poruka.

Edukacija i promišljenost

- Redovno pratite upozorenja, upoznajte se sa primerima prevara i delite informacije sa porodicom i prijateljima,
- Starije osobe su često meta – pomozite im da prepoznaju rizike,
- Ne ostavljajte broj telefona na javnim mestima bez potrebe,
- Ne dozvoljavajte aplikacijama pristup kontaktima ukoliko to nije neophodno.

Budite pažljivi kada odgovarate na poruke koje izgledaju sumnjivo

- Čak i poruke koje traže da se pošalje tekst ‘STOP’ kako ih više ne bi primali mogu poslužiti kao potvrda da je broj sa kog se odgovara aktivan.

Prijavljivanje prevare

- Prijava sumnjivih poruka se može uputiti Nacionalnom CERT-u i mobilnom operatoru
- Veb forma za prijavu Nacionalnog CERT-a: https://cert.rs/prijava.html
- Imejl adresa Nacionalnog CERT-a: info@cert.rs
- Dežurni broj telefona: 062 20 20 30