СМИШИНГ И РАЗВОЈ СМС ПРЕВАРА

Савремени ризици и мере заштите

РЕПУБЛИКА СРБИЈА
РАТЕЛ
РЕГУЛАТОРНА АГЕНЦИЈА ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ПОШТАНСКЕ УСЛУГЕ

СРБ-ЦЕРТ

www.cert.rs

Национални ЦЕРТ Републике Србије

Децембар 2025

Увод

Прва СМС порука послата је 3. децембра 1992. године, када је британски инжењер Нил Папворт са рачунара преко мреже „Vodafone GSM“ упутио свом колеги поруку „Срећан Божић“. Од тог тренутка СМС је постао симбол брзе и директне комуникације, али убрзо и средство које су нападачи почели да злоупотребљавају.

Све већи број превара одвија се путем СМС порука, које делују као званична обавештења од банке, курирске службе, државне институције, мобилног оператора, познатих дигиталних платформи као што су Netflix, Spotify и други стриминг или платни сервиси. Оне могу садржати злонамерне линкове, захтеве за личне податке, податке о платној картици или упутства која корисника доводе у ризик од преваре и губитка новца.

Смишинг (СМС фишинг) представља облик дигиталне преваре у ком преваранти шаљу СМС поруке које изгледају као званична обавештења, са циљем да наведу корисника да открије личне податке, податке са платне картице или да кликне на злонамерни линк.

У 2024. години Националном ЦЕРТ-у грађани су пријавили СМС преваре и укупан финансијски губитак у износу од приближно два милиона динара. Статистика којом располаже Национални ЦЕРТ заснива се на пријављеним случајевима СМС превара, па је важно напоменути да многе жртве превара нису пријавиле превару, али ни износ финансијског губитка, што значи да је стварна штета знатно већа од евидентиране. У току 2024. године све СМС преваре су биле усмерене на кориснике поштанских услуга.

Слика 1 - Пут од СМС поруке до крађе података

Први покушаји смишинга

У почетним годинама мобилне телефоније, СМС преваре су биле прилично једноставне. Најчешће су се сводиле на то да корисник позове број са високом тарифом или уплати припејд кредит на туђи рачун. Иако су такве поруке временом постале лако препознатљиве, и даље се користе као метод обмане.

Примери порука:

- „Освојили сте награду, јавите се на број…“
- „Ћао пишем ти са новог броја, молим те уплати ми допуну припејд кредита за овај број…“
- “Мама позови ме на овај број, изгубио сам телефон…”

Психолошки притисак као напредна тактика: хитност и страх

У последњих неколико година, СМС преваре су се трансформисале у смишинг кампање. Корисници су постајали све свеснији превара, па су преваранти почели да комбинују тактике хитности и страха. Развили су се аутоматизовани системи за слање порука великом броју корисника. Поруке долазе са бројева који изгледају као да су званични, а ликови воде ка уверљивим веб сајтовима који користе модеран дизајн.

Ове поруке садрже линкове ка лажним сајтовима који изгледају као странице банака, поште или државних институција. Често имитирају стил и садржај банке, курирске службе, државне институције, мобилне операторе или имитирају изглед познатих платформи као што су Netflix, Sportify и слично.

У порукама се налазе хитни позиви на акцију, а то код корисника изазива панику и брзу реакцију.

Примери порука:

- „Забележен је Ваш саобраћајни прекршај, кликните на линк да бисте платили казну“
- „Ваш пакет је задржан. Платите 150 дин за царињење да бисте добили пакет: [линк]“
- „Банка: ваш налог је привремено блокиран. Пријавите се овде да бисте могли да наставите да користите услуге банке: [линк]“
- „Netflix претплата није продужена. Потврдите картицу овде: [линк]“

Технолошки напредак: Злоупотреба идентитета пошиљаоца и смишинг кампање

Са порастом свести грађана о СМС преварама и злонамерни актери усавршавају своје методе. Једна од најопаснијих тактика је злоупотреба идентитета пошиљаоца, где порука изгледа као да долази од званичне институције, банке, мобилног оператора или познате платформе - иако то није случај.

Техника која се примењује у СМС преварама, у којој нападач којој нападач фалсификује идентитет пошиљаоца поруке како би преварио примаоца, се назива **СМС спуфинг** (енгл. SMS spoofing).

Зашто је ова тактика опасна?

- Корисник често не проверава пошиљаоца ако препозна име,
- Порука изгледа легитимно и не садржи очигледне грешке,
- Линк води ка страници која визуелно подсећа на званичну платформу.

Како се спроводи ова напредна СМС превара?

У свету мобилне комуникације, важно је разумети разлику између **P2P (Person-to-Person)** и **A2P (Application-to-Person)** порука, јер управо ова разлика игра кључну улогу у разумевању како се злоупотребљавају СМС поруке и настају СМС преваре.

P2P - Поруке између две особе

P2P комуникација подразумева размену СМС порука између два физичка лица. То су класичне поруке које шаљемо пријатељима, породици или колегама.

Карактеристике:

- Поруке се шаљу са мобилног броја на мобилни број,
- Не користи се код масовне дистрибуције,
- Не користе аутоматизоване системе,
- Углавном нису предмет злоупотребе у контексту СМС превара.

A2P - Поруке од апликација ка корисницима

A2P комуникација подразумева поруке које се шаљу од стране апликација у име банака, институција или платформи ка корисницима. То су поруке које добијамо као обавештења, потврде, кодове за пријаву или потврду, подсетници и слично.

Карактеристике:

- Поруке се шаљу са системских бројева или алфанумеричких пошиљаоца (нпр. „Netflix“, банка, Пошта Србије),
- Често користе аутоматизоване системе за масовну дистрибуцију,
- Могу садржати линкове, кодове, позиве на одређене активности,
- Ово је начин комуникације који преваранти злоупотребљавају - имитирајући званичне пошиљаоце и садржај.

Зашто је важно разликовати?

Поруке које изгледају као A2P, али долазе од превараната, могу лако да наведу корисника да кликне на линк, унесе податке или изврши уплату. Зато је важно да грађани знају да:

- Званичне институције ретко траже личне податке путем СМС-а,
- Пошиљалац се може лажно приказати као званичан,
- Лажне A2P поруке се често користе у смишинг кампањама.

За A2P комуникације постоје апликације уз помоћ којих може да се унесе било који текст, број или њихова комбинацију у поље за идентификацију пошиљаоца, то је алфанумерички назив односно „Sender ID“.

Карактеристике:

- Убацивање лажних порука у постојећи низ,
- Манипулација Sender ID-ом,
- Технике које користе контекст и време (нпр. након праве поруке од курирске службе).

Примери:

- Лажни назив пошиљаоца (Sender ID): Уместо броја, порука се приказује као да је стигла од Поште Србије, банке, од NETFLIX-а или оператора, што код корисника изазива поверење,
- Убацивање у постојећи низ порука: Злонамерни актери понекад успеју да порука изгледа као део претходне комуникације са институцијом, што додатно отежава препознавање преваре,
- Изглед поруке: Формулације, правопис и визуелни стил поруке имитирају званичне шаблоне, укључујући логое, потписе и линкове који личе на праве адресе.

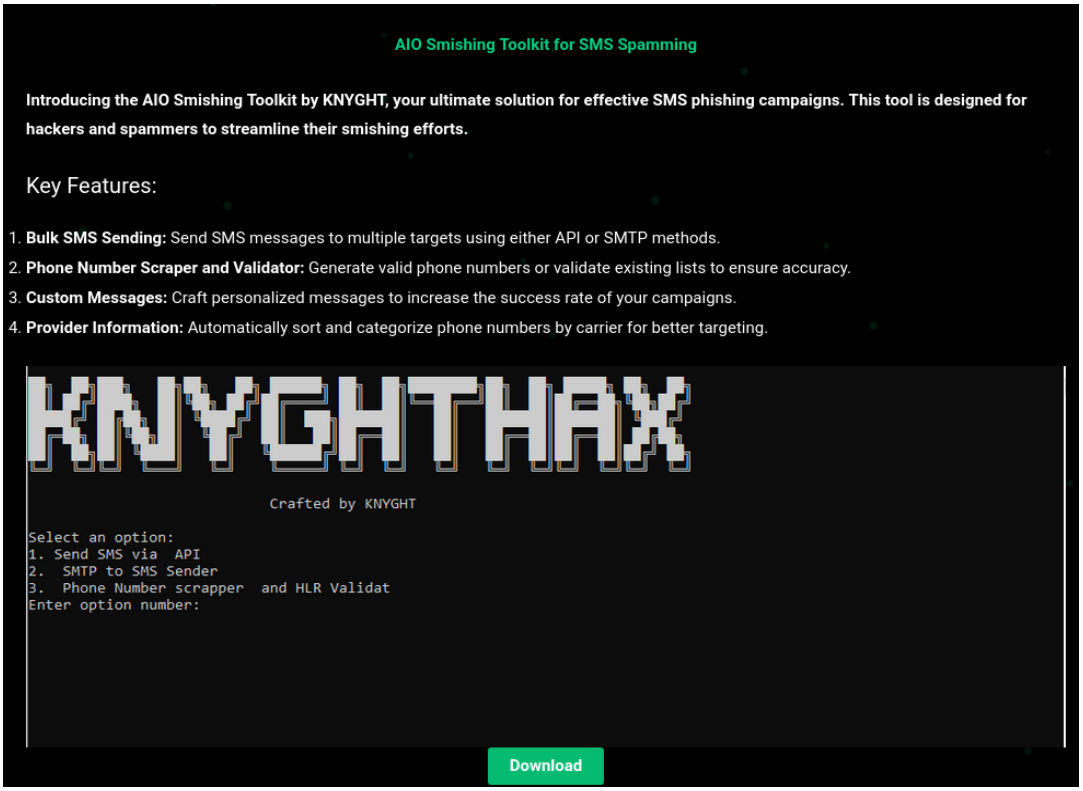
AIO (all-in-one) софтверски алати за смишинг нападе

Нападачи користе специјализоване алате AIO (all-in-one) за аутоматизоване смишинг нападе који омогућавају масовно слање лажних СМС порука и крађу података уз минималан труд. Ови алати комбинују више функција у једној платформи, чинећи их изузетно ефикасним и опасним. Омогућавају аутоматизацију напада и масовно слање лажних СМС порука корисницима широм света, лажно представљање као банке, курирске службе, државне институције уз адекватан превод на језик корисника.

Пример алата за смишинг, познат као „AIO Smishing Toolkit“, приказан је на Слици бр. 2. Овај софтверски пакет омогућава нападачу да:

- масовно шаље СМС поруке на више бројева, користећи различите техничке методе
- провери да ли су бројеви телефона активни и важећи, чиме се избегавају неуспешне испоруке,
- формулише персонализоване поруке ради повећања уверљивости и ефикасности напада,
- сортира и категорише листу бројева према мобилном оператору, што омогућава прецизније таргетирање жртава.

Овакви алати показују колико су данашње СМС преваре технички напредне и зашто је важно да грађани буду информисани и опрезни.



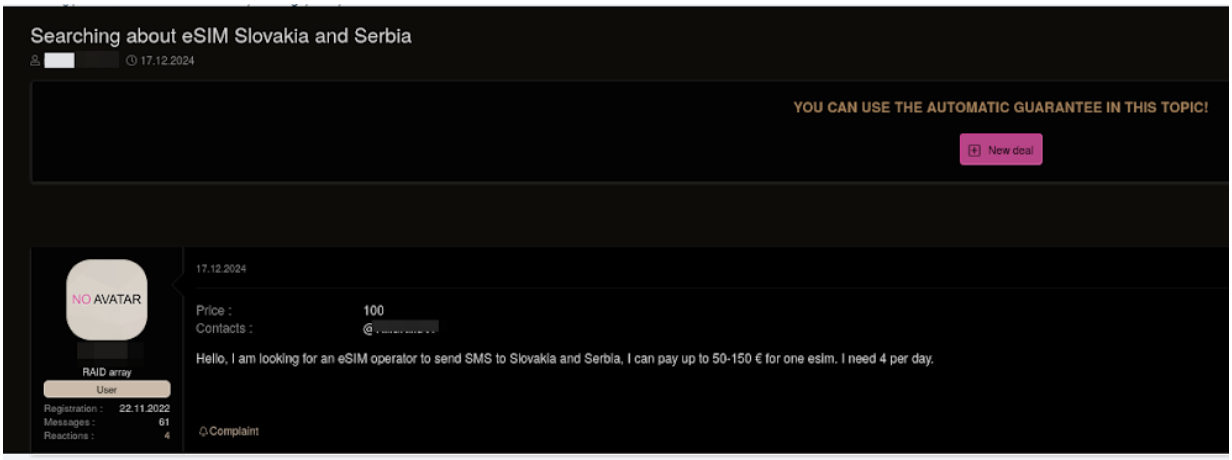
Слика 2 - Алат за реализацију смишинг напада

Нападачи долазе до бројева телефона путем различитих извора, често нелегалних, који им омогућавају да масовно шаљу смишинг поруке. Базе података које садрже податке грађана најчешће купују на црном тржишту.

Те базе потичу из:

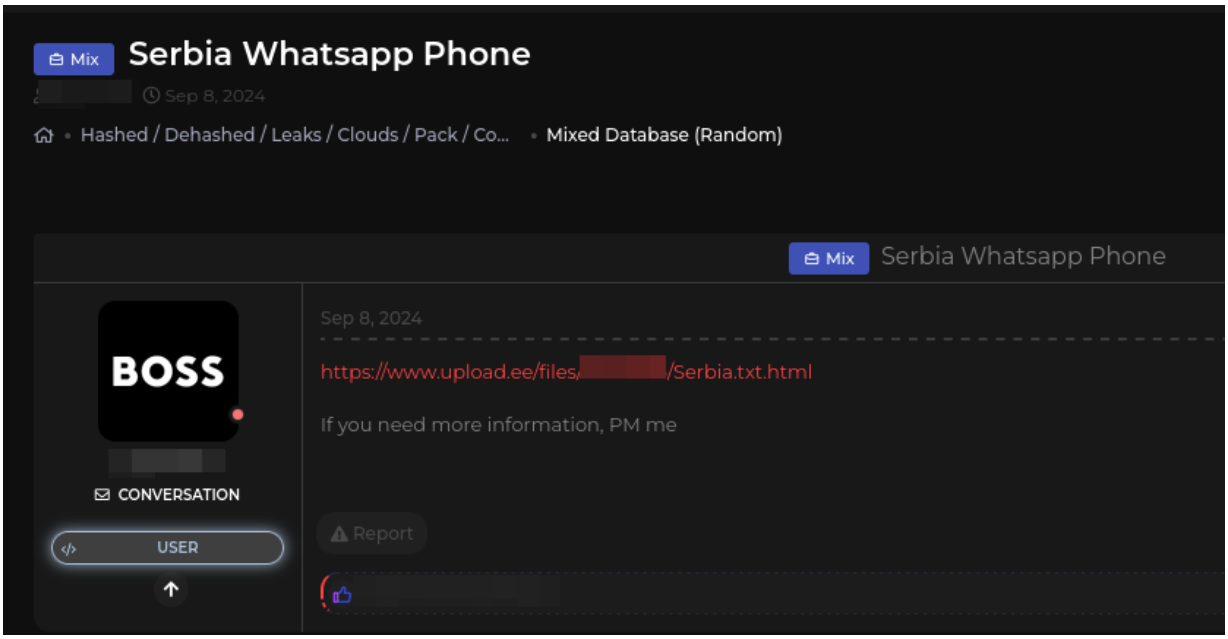
- украдених података са платформи за е-трговину, на којима грађани остављају податке,
- незаштићених онлајн формулара,
- путем апликација које траже дозволу за приступ контактима на мобилном телефону,
- из јавних извора (огласи, друштвене мреже, форуми где корисници остављају контакт).

На слици бр. 3 приказана је форумска порука са дарк веба, у којој корисник тражи еСИМ картице за слање СМС порука ка Србији. Пост је објављен 17. децембра 2024. године, а корисник је регистрован крајем новембра 2022. године. У поруци се наводи да је спреман да плати 50 до 150 евра по једној еСИМ картици, да му је потребно четири картице дневно и да жели да шаље СМС поруке ка наведеним државама. Ова слика указује на постојање тржишта, на форумима који нису јавни или званични, за набавку еСИМ ресурса у сврху масовног слања СМС порука, што може бити повезано са смишинг кампањама или другим облицима злоупотребе мобилних комуникација.



Слика 3 - Форумска порука са дарк веба

На слици бр. 4 је пример форумске размене података и бројева мобилних телефона који могу бити злоупотребљени у смишинг кампањама. Приказан је пост са онлајн форума под називом „Serbia Whatsapp Phone“, у оквиру категорије „Mixed Database [Random]“. Пост је објављен 8. септембра 2024. године. У садржају поруке налази се линк ка датотеци под називом „Serbia.txt.html“, која је хостована на спољној платформи за дељење фајлова. Опис теме и ознаке („Hashed / Dehashed / Leaks / Clouds / Pack…“) указују да се ради о потенцијално компромитованим подацима, вероватно телефонским бројевима повезаним са WhatsApp корисницима у Србији. Ово је и пример како се лични подаци могу наћи на дарк вебу и зашто је важно да грађани буду опрезни са дељењем броја телефона и активностима на мобилним апликацијама.



Слика 4 - Пример објаве са дарк веба: дељење листе бројева из Србије

Нова генерација СМС превара: Поруке које се настављају на легитимне у истом низу

Савремене СМС преваре више не изгледају као поруке од непознатих бројева са лошим правописом. Напротив, преваранти користе технички напредне методе које поруке чине уверљивим, временски усклађеним и визуелно идентичним званичним обавештењима.

Једна од најопаснијих тактика је убацивање лажне поруке у постојећу преписку са банком, курирском службом или мобилним оператером. Корисник види поруку у истом низу као претходне званичне поруке, што ствара утисак да је и нова порука поуздана.

Корисници често имају навику да верују порукама које стижу у већ постојеће преписке са институцијама, па је овај облик напада посебно опасан. Због тога је важно да се увек провери садржај поруке, да се не приступа сумњивим линковима, као и да се информације потврде директно преко званичних апликација или интернет страница.

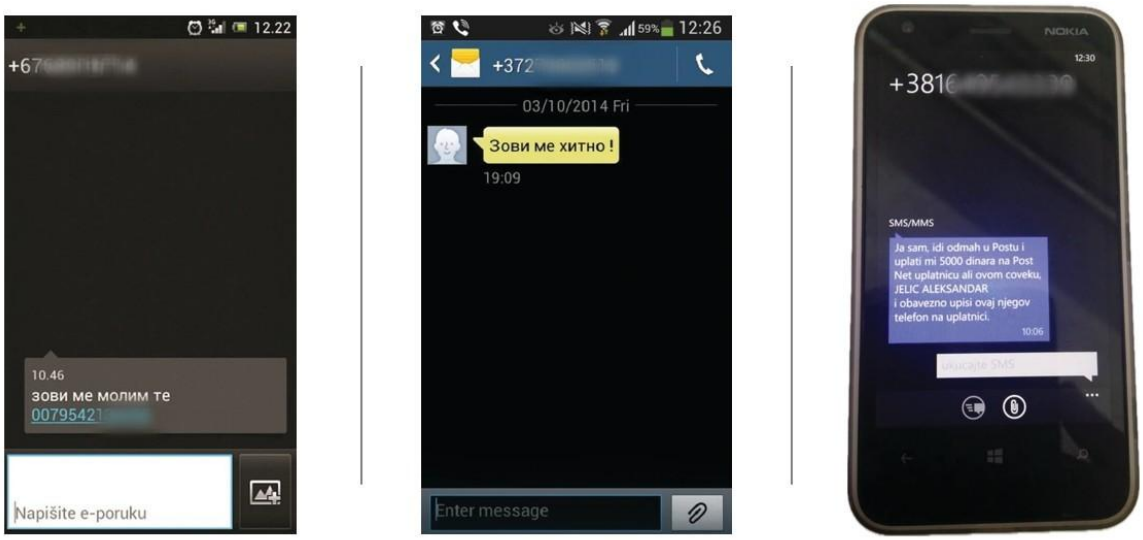
Нападачи то постижу тако што намерно манипулишу пољем Sender ID. У пракси, они најчешће злоупотребљавају слабо заштићене СМС gateway-е и A2P апликације у којима могу да подесе идентификатор пошиљаоца по жељи. На тај начин порука изгледа као да је стигла од банке или друге институције. Мобилни телефони све поруке групишу управо по том идентификатору, па систем не прави разлику између легитимне и лажне поруке ако обе носе исти Sender ID. На тај начин, корисничка апликација у мобилним телефонима приказује све поруке у једном низу, што превару чини уверљивом и тешком за препознавање.

Ређи и технички сложенији случај је злоупотреба SS7 протокола који омогућава размену сигнализационих порука између мобилних мрежа.

Примери СМС превара

Први покушаји смишинга

Класичне СМС преваре имају примаран циљ да наведу примаоца да реагује: да одговори, позове број или да следи инструкције које доводе до финансијског губитка. Поруке обично стижу са непознатих бројева и садрже лажне, али уверљиве информације.



Слика 5 - Примери класичних превара

Важно је остати опрезан и не реаговати импулсивно на поруке које делују хитно или необично. Треба увек прво размислите о садржају поруке пре предузимања било какве акције.

Пошта Србије

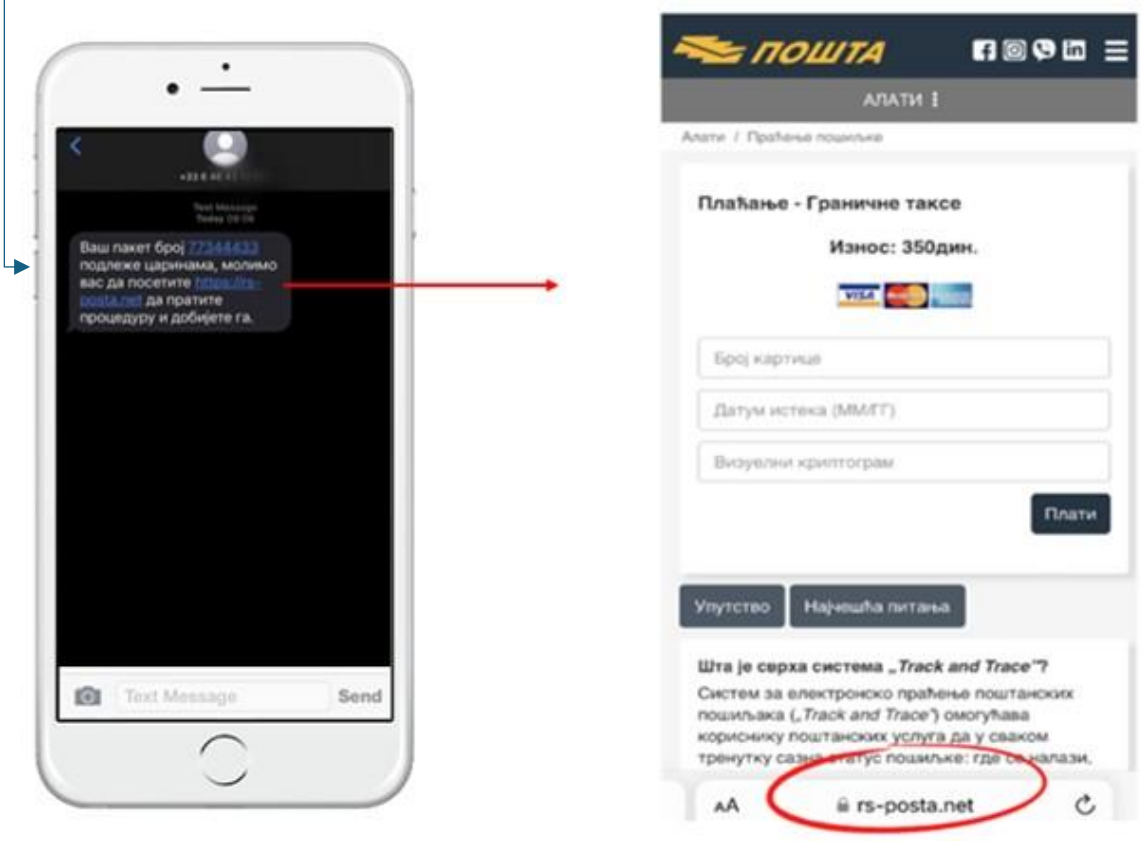
Корисницима се шаље лажна СМС порука да им наводно пакет није могао бити испоручен због неплаћене царине и да за испоруку треба отворити линк из поруке.

Примери лажних линкова:
https://rs-posta.com
https://rs-posta.net
https://posta-serbia.com
https://posta-srbija.com

Легитиман линк:
https://www.posta.rs/

Ваш пакет број 77344433 подлеже царинама, молимо вас да посетите

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

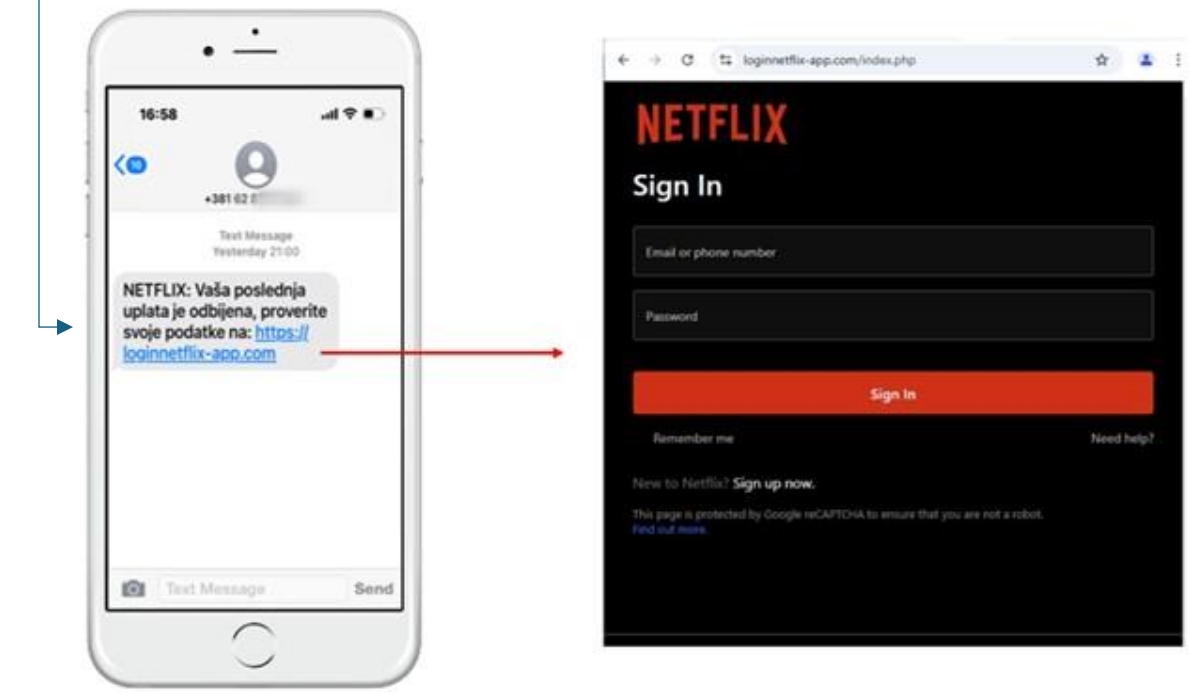


Слика 6 - Превара која се односи на Пошту Србије

Netflix превара

Преваранти шаљу поруку која изгледа као обавештење од Netflix-а, а линк води ка лажној страници за пријаву. Уносом података, корисник несвесно открива своје поверљиве информације.

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



Слика 7 - Превара која се односи на Netflix

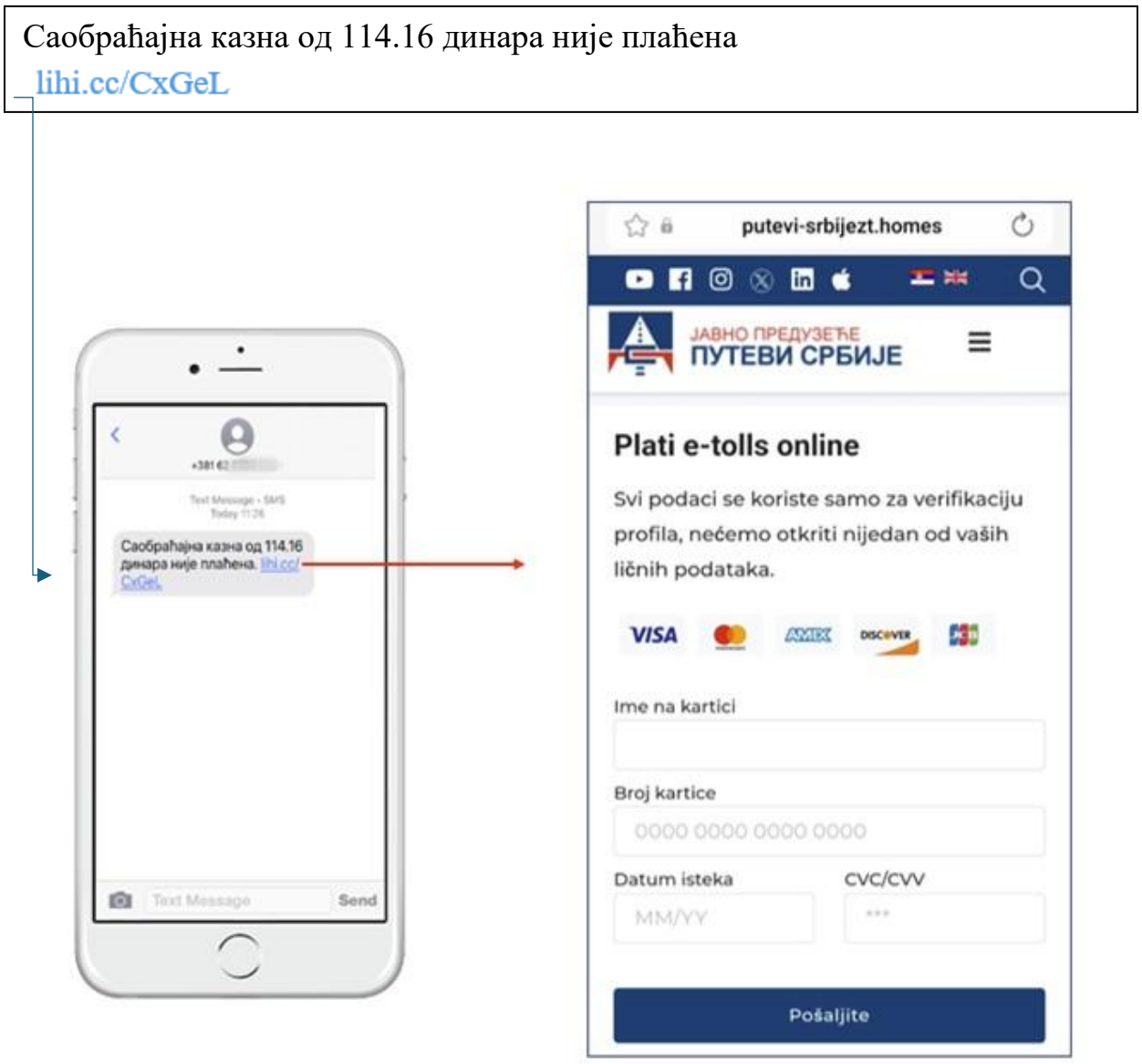
Шта овај пример показује:

- СМС порука: изгледа званично али садржи позив на акцију и линк који није званичан,
- Лажна страница: имитира Netflix, али URL није званичан

  (нпр. *https://loginnetflix-app.com* уместо званичног *https://www.netflix.com*),
- Ризик: уносом података, корисник омогућава приступ налогу или подацима са платне картице.

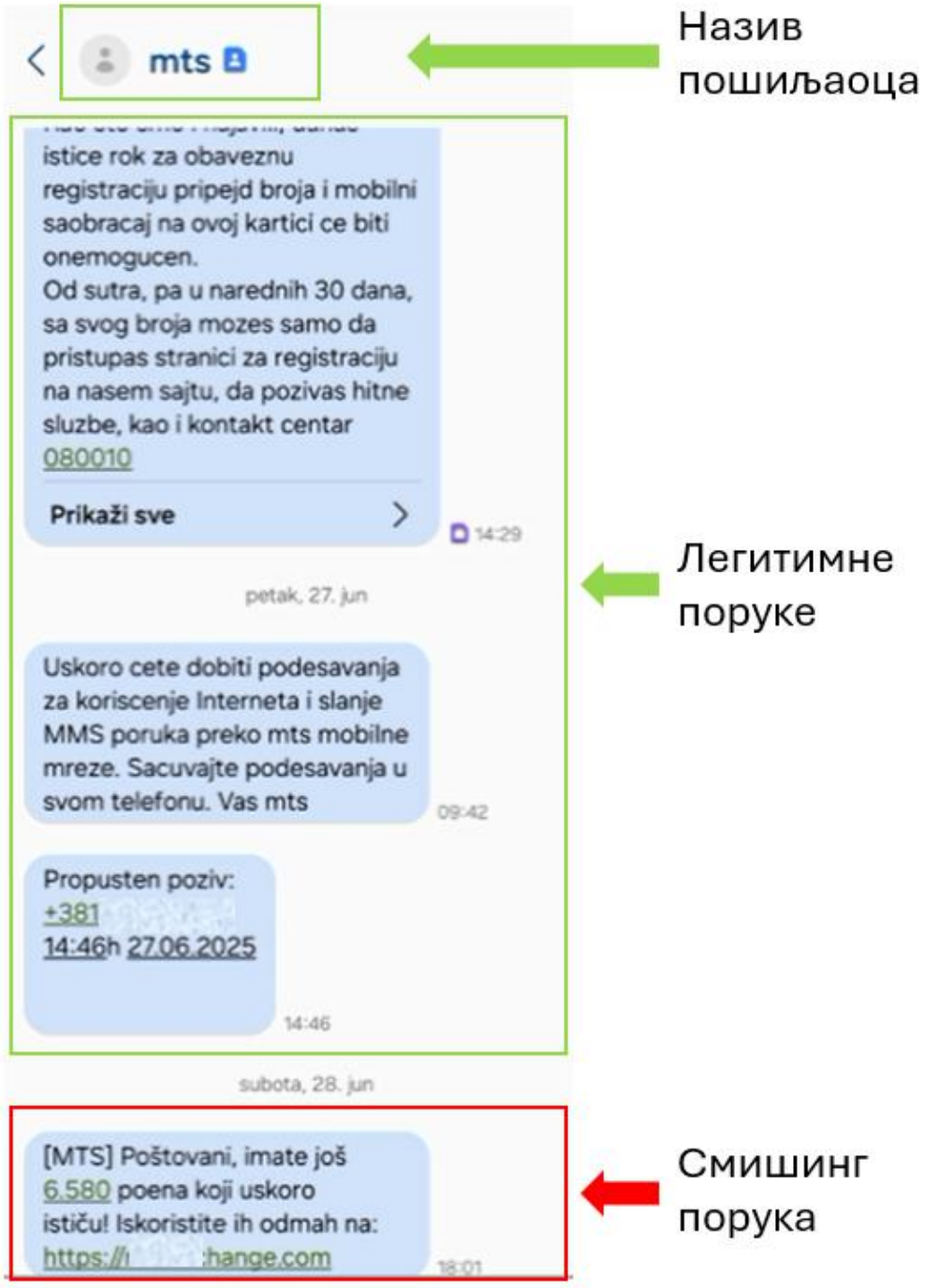
Путеви Србије

У смишинг кампањи која је усмерена на Путеве Србије, нападач се лажно представља као „ЈП Путеви Србије". У тим порукама се наводи да је прималац начинио саобраћајни прекршај или није платио путарину, уз позив да преко приложеног линка изврши уплату. Линк води ка лажној интернет страници која опонаша званичну институцију, а крајњи циљ је да се грађани наведу да унесу податке са своје платне картице, чиме се омогућава злоупотреба, односно крађа новца.



Слика 8 - Превара која се односи на Путеве Србије

Пример преваре путем СМС поруке која се појављује у легитимном низу порука



Слика 9 - Смишинг поруке које се настављају у истом низу на легитимне

Од кључне је важности да корисник не реагује импулсивно. Пре било какве акције, потребно је пажљиво проверити ко је пошиљалац и шта порука заиста садржи. Само опрезом и критичким размишљањем можемо се заштитити од оваквих обмана.

Мере заштите

Обазриво приступајте порукама које траже хитну акцију

- Ако се у поруци тврди да морате одмах да кликнете на линк, платите казну, потврдите идентитет или унесете адресу за доставу пакета - будите сумњичави.

Препоручује се опрез при приступу сумњивим линковима

- Линкови у порукама могу водити ка лажним сајтовима који изгледају као банке, поште или курирске службе,
- Уместо клика отворите званичну веб страницу или позовите контакт центар.

Избегавајте унос личних података путем СМС-а

- Проверите да ли је пошиљалац заиста званичан - институције ретко шаљу линкове путем СМС-а,
- Банке, државне институције и курирске службе никада неће тражити ПИН, лозинку или податке са платне картице путем поруке,
- Не уносите податке преко линкова из порука, већ директно преко званичног сајта.

Користите апликације за заштиту мобилних уређаја

- Активирајте опције за блокирање или филтрирање непознатих пошиљаоца,
- Ако сте у могућности инсталирајте верзију антивирусне апликације која има заштиту од смишинг порука.

Едукација и промишљеност

- Редовно пратите упозорења, упознајте се са примерима превара и делите информације са породицом и пријатељима,
- Старије особе су често мета - помозите им да препознају ризике,
- Не остављајте број телефона на јавним местима без потребе,
- Не дозвољавајте апликацијама приступ контактима уколико то није неопходно.

Будите пажљиви када одговарате на поруке које изгледају сумњиво

- Чак и поруке које траже да се пошаље текст ‘СТОП’ како их више не би примали могу послужити као потврда да је број са ког се одговара активан.

Пријављивање преваре

- Пријава сумњивих порука се може упутити Националном ЦЕРТ-у и мобилном оператору
- Веб форма за пријаву Националног ЦЕРТ-а: https://cert.rs/prijava.html
- Имејл адреса Националног ЦЕРТ-а: info@cert.rs
- Дежурни број телефона: 062 20 20 30